TELECOMMUNICATIONS SECURITY

IPUT

About INPUT

INPUT provides planning information, analysis, and recommendations to managers and executives in the information processing industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions. Continuing services are provided to users and vendors of computers, communications, and office products and services.

The company carries out continuous and in-depth research. Working closely with clients on important issues, INPUT's staff members analyze and interpret the research data, then develop recommendations and innovative ideas to meet clients' needs. Clients receive reports, presentations, access to data on which analyses are based, and continuous consulting.

Many of INPUT's professional staff members have nearly 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed in 1974, INPUT has become a leading international planning services firm. Clients include over 100 of the world's largest and most technically advanced companies.

Offices

NORTH AMERICA

Headquarters
1943 Landings Drive
Mountain View, CA 94043
(415) 960-3990
Telex 171407

New York
Parsippany Place Corp. Center
Suite 201
959 Route 46 East
Parsippany, NJ 07054
(201) 299-6999
Telex 134630

Washington, D.C.
11820 Parklawn Drive
Suite 201
Rockville, MD 20852
(301) 231-7350

EUROPE

United Kingdom
INPUT
41 Dover Street
London W1X 3RB
England
01-493-9335
Telex 27113

Italy
Nomos Sistema SRL
20127 Milano
Via Soperga 36
Italy
Milan 284-2850
Telex 321137

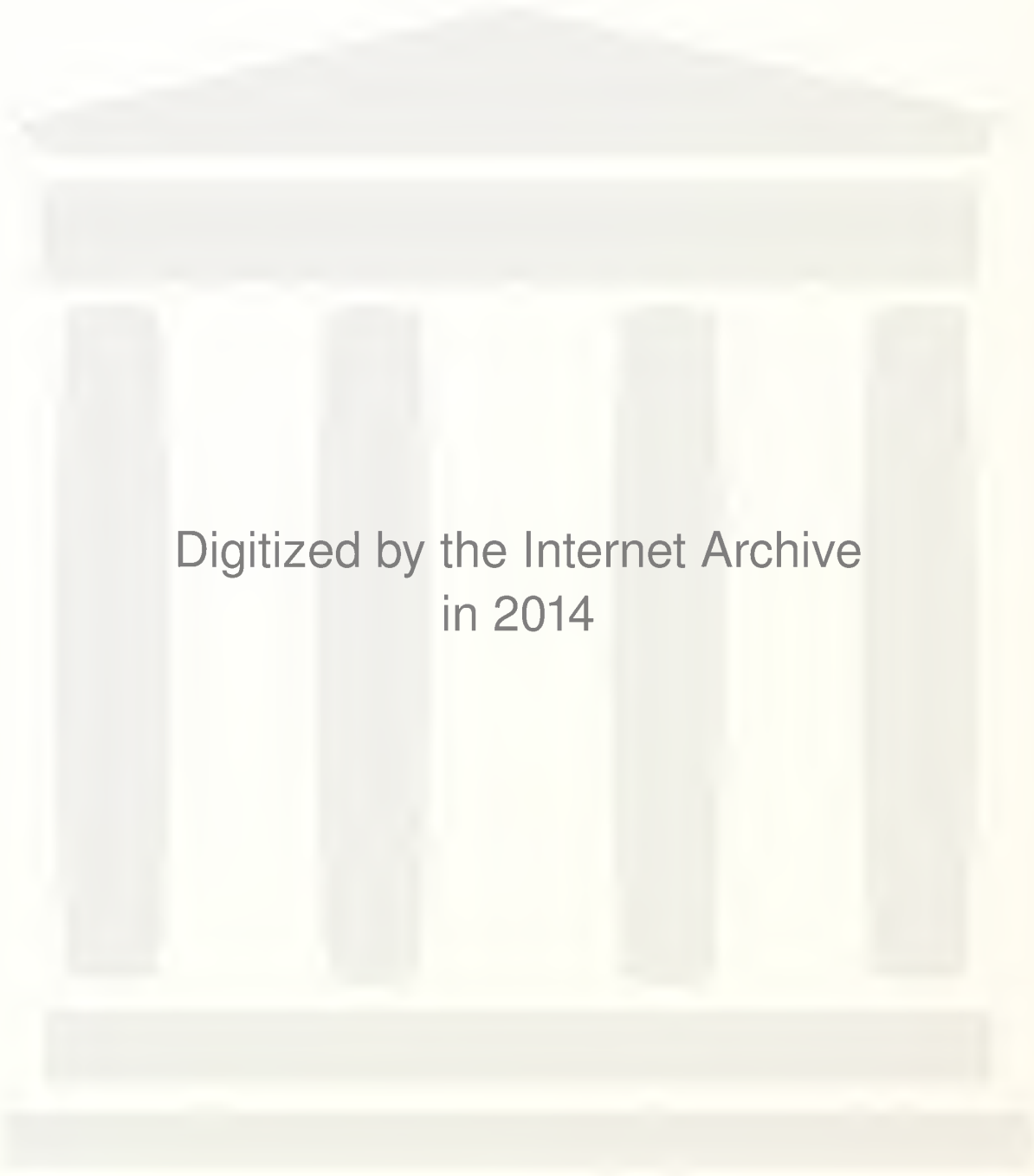
Sweden
Athena Konsult AB
Box 22232
S-104 22 Stockholm
Sweden
08-542025
Telex 17041

ASIA

Japan
ODS Corporation
Dai-ni Kuyo Bldg.
5-10-2, Minami-Aoyama
Minato-ku,
Tokyo 107
Japan
(03) 400-7090
Telex 26487

INPUT®
Planning Services For Management

TELECOMMUNICATIONS SECURITY



TELECOMMUNICATIONS SECURITY

ABSTRACT

This report was produced as part of INPUT's Telecommunications Planning Program. It describes the current state of security within both data processing and telecommunications. This report examines and analyzes the breadth and limitations of current technology, analyzes the requisite functional areas, and describes the efforts and effects of a national data encryption standard. The report concludes with a series of recommendations for future planning purposes.

This report contains 184 pages, including 22 exhibits.

TELECOMMUNICATIONS SECURITY

CONTENTS

EXHIBITS

1 INTRODUCTION

I INTRODUCTION

- This report is part of INPUT's Telecommunications Planning Program. Designed to apprise senior and middle managers and executives of the basic issues relating to data and communications security, this report identifies interim solutions to overall systems security and assessess opportunities associated with the technology of telecommunications security. In additon, this report:

  - Identifies technological data and telecommunications requirements.

  - Defines and analyzes the current and projected state-of-the-art of systems security.

  - Analyzes the major market products associated with systems security.

  - Identifies the thrust and direction of growth and development relating to data and telecommunications security.

  - Defines the basic requirements of a secure data transmission system and proposes a number of implementation techniques toward building secure telecommunications systems.

A. PURPOSE AND SCOPE

- Over the years data processing and communications users have had a primary concern over the maintenance of the integrity of their data, whether for processing or transmission or for both.

- Data integrity in this case means the true representation of information and the transmission of information without alteration or errors.

- Numerous error detection and correction techniques have been developed and are implemented today to validate the transmission of information over communications lines, as well as validate the transmission of information between co-located computers and the various components of a data processing system.

- The same techniques used by the government, particularly the military, are now being adapted for commerce and industry in order to assure the timely, correct, error-free transmission of information and data.

- For managers and executives involved in information systems or communications management, it is becoming incumbent upon them to be aware of the issues and problems relating to systems security and to understand the methodologies, techniques, and solutions relating to existing or anticipated security activities.

- In support of these processes, this report;

  - Examines the major factors involved in systems security and their application in a data processing and/or transmission environment.

  - Evaluates some of the problems, opportunities, and costs associated with the data transmission process.

- Describes the role of data encryption and describes how and why it is coming into wider use.

- Provides insights into how some large organizations have handled the problem and possibilities of transmission security.

- For purposes of this report, the term "telecommunications" will be taken to include both voice and data transmissions.

B. REPORT ORGANIZATION

- This report is organized along the following lines:

  - Chapter I is an introduction.

  - Chapter II is an Executive Summary. It is formatted as a presentation for group discussions and emphasizes the key points within the report.

  - Chapter III examines some of the security issues from a management point of view. It also identifies some of the considerations affecting the implementation and utilization of a data and/or telecommunications security system.

  - Chapter IV evaluates the present state of the technology with particular emphasis on transmission security and integrity.

  - Chapter V evaluates the issues relating to data base security and identifies some of the weaknesses and strengths of some representative systems.

- Chapter VI contains the conclusions and INPUT's recommendations for designing, implementing, and using an effective data security and telecommunications transmission system.

- Appendix A contains a survey of some of the software products that might be of interest to the user community.

- Appendix B briefly describes some of the hardware considerations as adjuncts to software security activities.

- Appendix C contains the questionnaire used to conduct the interviews.

C. METHODOLOGY

- The information for this report was generated from the following sources:

  - Structured interviews were conducted with key personnel in a number of large companies currently using or planning to use some form of data and/or telecommunications security.

  - Additional in-depth interviews took place with leading vendors and suppliers of software and hardware products that might be required in building a secure data processing or telecommunications system.

  - INPUT's own studies into data security and telecommunications integrity were analyzed.

  - Vendor-supplied product literature and other secondary research sources were analyzed.

D. OTHER RELATED INPUT REPORTS

- Telecommunications Strategic Planning (1984).

  - This report discusses strategic methodologies and telecommunications planning principles with particular emphasis on the consequences of strategic planning.

- Telecommunications Interfaces for the Mid-1980s (1984).

  - Defines and identifies the problems and some proposed solutions relating to interconnect data and telecommunications devices. It also defines some of the relevant architectures and protocols that bear directly on security issues.

- Network Management and Control Systems (1984).

  - An in-depth analysis and review of management control problems and solutions, especially as they relate to network control systems design and implementation.

- SNA Network: Challenges and Opportunities (1984).

  - This report describes and then discusses in detail the IBM System Network Architecture product offerings with particular emphasis on how and why this architecture is utilized.

II EXECUTIVE SUMMARY

II EXECUTIVE SUMMARY

- This Executive Summary is designed in a presentation format in order to:
  - Help the busy reader quickly review key research findings.
  - Provide a ready-to-go executive presentation, complete with a script, to facilitate group communication.
- Key points of this report are summarized in Exhibits II-1 through II-6. On the left-hand page facing each exhibit is a script explaining the contents of the exhibit.

A. BASIC DEFINITIONS

- Data security has been defined as the protection of data from either accidental or intentional disclosure to or by unauthorized persons, or from authorized modification.

- Telcommunications security may be defined as the transmission of true and accurate data via telcommunication links or devices to the receiving party or place in unaltered or unmodified form.

- Data security includes (but is not limited to):

  - Computer hardware features.

  - Programmed routines.

  - Manual computer procedures.

  - Physical safeguards; e.g., locks, keys, badges, etc.

- Telecommunications security includes (but is not limited to):

  - Communications equipment.

  - Communications links and lines.

  - Data transmission devices; e.g., modems, terminals, multiplexes, etc.

  - Supporting software and firmware.

INPUT®

BASIC DEFINITIONS

- **Data Security**
  - **Perfect Data**
    - **Hardware**
    - **Software**
    - **People**
    - **Fences**

  Telecommunications Security

  - **Accurate Transmission**
    - **Hardware**
    - **Software**
    - **Firmware**
    - **Lines, etc.**

B. COST/PROTECTION/COMPLEXITY TRADEOFFS

- As the extent of data communications goes up, so does the complexity of the security environment.

- As the degree of protection increases, so does the cost. These increases are usually in direct proportion.

- As the organization approaches perfect security, the user may find that he has built himself a prison whereby no one will (or can) work in that environment and/or no work will be done.

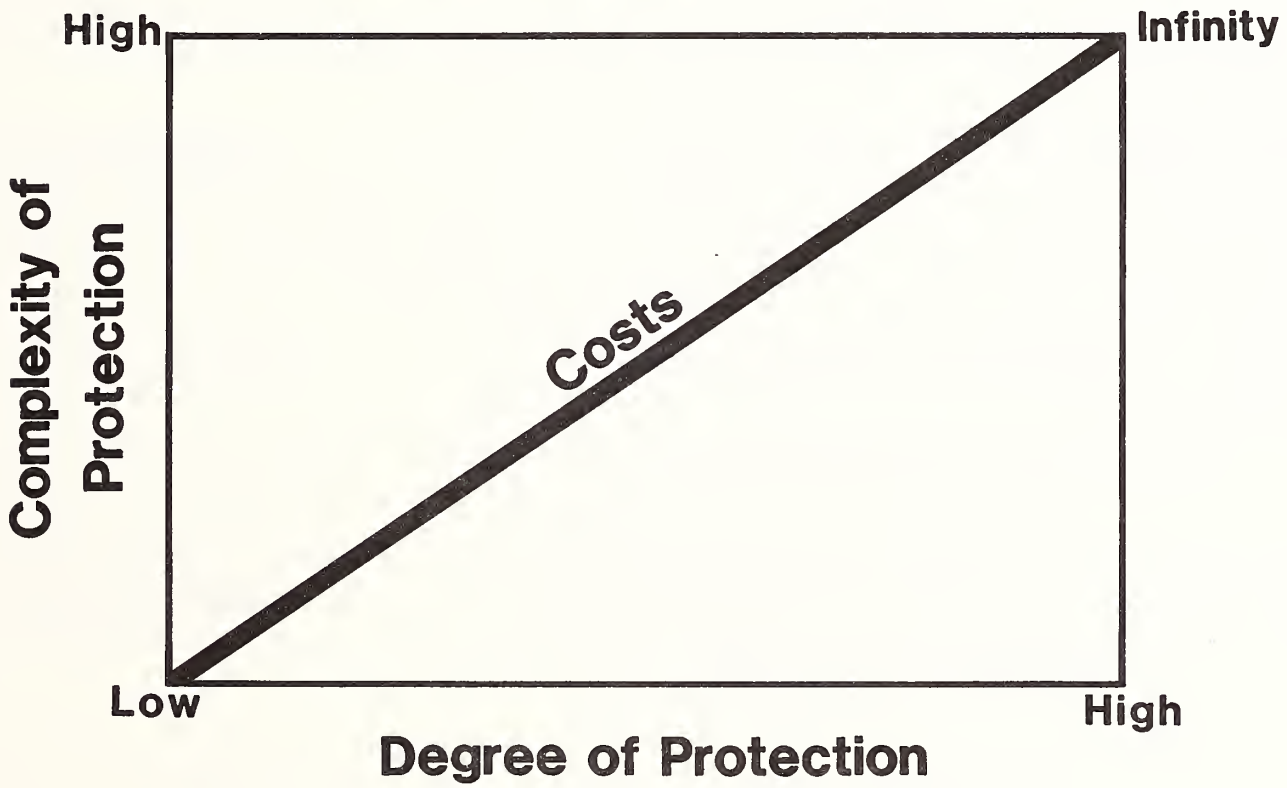
  - Thus, it becomes apparent that while it might be theoretically possible to have perfect security, who can afford to pay the personnel and economic costs?

  - Planning managers should realize that to constrain the creative programmer or communications technician by excessive security restrictions will negate the very factors that make his contributions cost-effective--creativity.

    . The operative word is "excessive."

    . How much security is "excessive" depends on the company, its goals, and its workers (and what they think).

COST/PROTECTION/COMPLEXITY TRADEOFFS



C. SOME REPRESENTATIVE HAZARDS

- Some of the techniques used to intercept or otherwise alter transmissions include the following:

  - Trojan Horse - This involves tricking persons or programs with legitimate systems access into doing things that they would not normally do.

  - Trap Door - This is an implicit mechanism within the operating system to perform a normally privileged function.

  - Booby Trap - This is usually a program that works on the principle of a bank vault: at a certain time or under certain predetermined conditions, the program will automatically execute, usually in combination with another legitimate program.

  - Salami Section - This is usually a software subroutine that is unknowingly involved at every execution of some frequently run program. Where money is involved, it only takes small amounts, preferring the high frequency of program executions to affect the theft rather than a single, large transaction.

  - Time Bomb - This is an algorithm built into a program that only executes at some future, predetermined time. Usually its purpose is malicious damage rather than personal gain. However, many softwre manufacturers use it to enforce license or lease agreements.

  - Piggyback - This technique allows an unauthorized user to enter the system via a legitimate user's sign-on or access procedure. Frequently used by "hackers," it is sometime very difficult to detect.

INPUT®

SOME REPRESENTATIVE HAZARDS

• Trojan Horse	• Tricks Users
• Trap Door	• Performs Normal Functions, Using Deceit
• Time Bomb	• Invoked at Some Predetermined Time
• Piggy Back	• Unauthorized Access on Legitimate Usage

D. SYSTEM DESIGN CONSIDERATIONS

- A security system must be modular so procedures can be tailored to user needs and enforced in appropriate access.

- Factors which influence the design of a secure data communications system include:

  - Information Content, where data may require no special security provisions, normal need-to-know restrictions, or extensive precautions to avoid disclosure.

  - Environment, where users may be all on-line, all off-line, or any combination; or have equal or widely varying security clearance levels.

  - Communications, where devices and activities may be local (within same building or complex); dedicated, private network; or switched network.

  - System Facilities, where services provided may be dedicated function only (inquiry or data entry), interactive - problem solving, full remote programming and testing support, or total information system.

INPUT®

SYSTEM DESIGN CONSIDERATIONS

- Information Content
- Environment
- Communications
- System Facilities

E. BEWARE: DON'T OVERSECURE

- Data is a physical asset in any organization. Protect it and control it!

- Remember, security is a broad topic with many ramifications; it is too broad to cover completely with this single report.

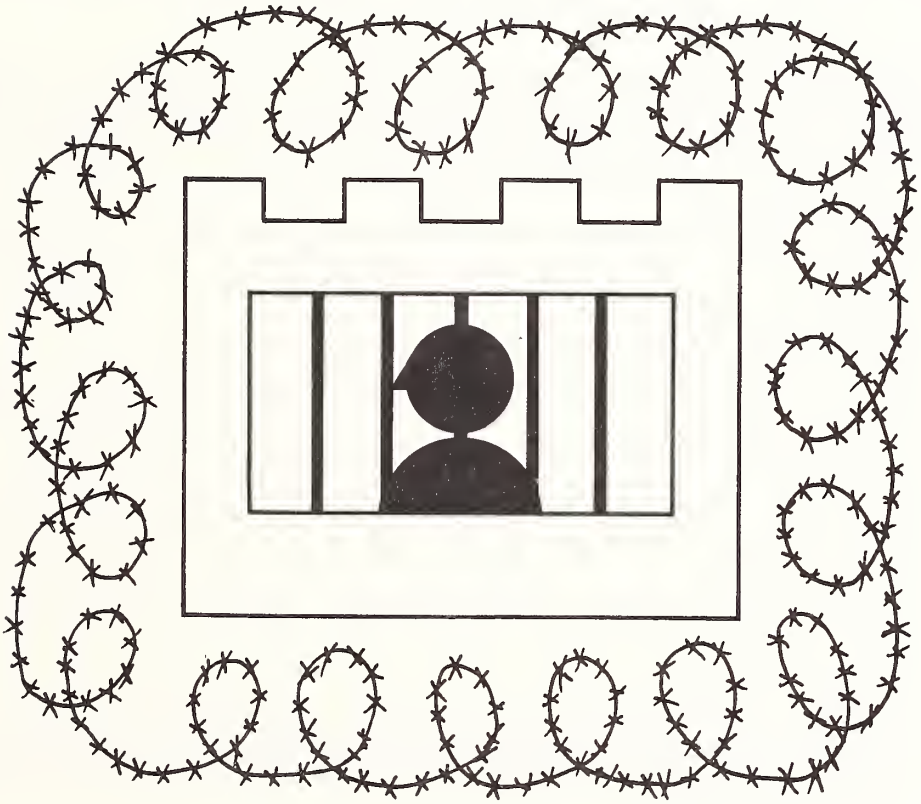
  - Its complexity requires the utmost consideration to the needs of the organization versus the needs to get the job done.

  - Overzealous or overdesigned security systems resemble prisons, which rapidly become prisons of the mind.

    . Judgement and discretion is required when designing or implementing such systems.

  - And finally, people need to perform useful work if the organization is to succeed. Too much security could make productive effort an exercise in futility. Don't let that happen in your shop.

BEWARE: DON'T OVERSECURE



F. RECOMMENDATIONS

- The manager should try to adopt as many techniques of telecommunications and data security as he and his staff feel comfortable with. There should be sufficient security to get the job done, but not so much that it interferes with the ability or privacy rights of the contributing technical staff.

- Judgement is the key to good security practices. By all means, protect the organization's asset base, but remember, people still need to get the job done. Thus, the product manager will not put up a fence around his people so that they cannot tolerate the working environment.

- Every manager should ask himself two basic questions:

  - How little (not how much) security do I really need?

  - How will security impact my ability to get my job done through the efforts of others.

- The role of the "hacker" who breaks into computer systems may be over-emphasized. Usually hackers break in for intellectual challenge, not for malicious reasons.

  - Once inside the system, the hacker usually doesn't know what to do since he usually doesn't understand either the architecture or the configuration.

  - Fairly simple log-ons recording software will usually indicate the presence of a "hacker."

INPUT®

RECOMMENDATIONS

- Use Available Techniques with Discretion
- Judgment is the Key
- Ask the Basic Questions
  - How Little is Needed?
  - What is the Impact?
- Weigh Carefully the Value of Security
- Hackers are not the Problem

III MANAGEMENT CONSIDERATIONS

III MANAGEMENT CONSIDERATIONS

A. MANAGEMENT OVERVIEW

- Major managerial control issues include the questions:
  - Who should be authorized?
  - How is this determined?
  - How is the authorization process operated?
- In recent years various authorities have attempted to address some of these policy and procedural issues.
- With few exceptions, these studies either have been imbedded within elaborate privacy or technical security reports or have been intended to serve as introductions to particular aspects of the problem area.
  - As a result, the literature on managerial security is largely diffused and unorganized.
  - This report introduces a comprehensive framework for organizing and studying the diverse aspects of managerial security. This framework places issues of management policies and procedures into four categories:

- Operational considerations.
- Organizational impact.
- Economics.
- Objectives and accountability.

- Using this framework, the key issues regarding management policies and procedures for effective computer security are categorized and analyzed. Specific emphasis is placed on proposals regarding surveillance and authorization.

I. OPERATIONAL CONSIDERATIONS

- Many managerial decisons must be made regarding the procedures to be used in the operation of an organization's computer facility. Although most of these decisions are intended primarily to increase the degree of data security, they must also be viewed in light of the organization's overall objectives.

a. Operational Environment

- Physical and operational procedures can be used to limit significantly the number of people that have any access to the computer facility. The three major categories of access are:

  - Closed. Only a very small number of operators have direct access to the computer facility. All computation to be performed is submitted to one of the operators who will then oversee the actual run.

  - Open. In principle, any member of the organization may have access to the computer facility. The user must physically appear at the

computer facility to perform computations and may be screened at that time.

- Unlimited. Access to the computer facility is via communication lines. usually the public telephone network. The user need not ever physically appear at the computer facility or have any personal contact with the operators of the facility.

- There are, of course, variations on the operating environments listed above. Each environment has implications for the organization's data security as well as the utility of the computer facility.

- By severely limiting access, such as in a closed environment, controls similar to those used for a bank vault can be enforced. In fact, most high security military installations use this approach and the "computer room" is often actually a vault.

  - Although a closed environment can provide high physical security, it may not be consistent with the organization's needs.

  - Many of the important modern applications of computers are dependent upon the concept of on-line access - leading essentially to an unlimited access environment.

- The open and unlimited access environments introduce different types of risks.

  - In an open environment it is possible to screen out external intruders, but the computer facility is still exposed to the actions of internal users who have legitimate physical access to it.

  - An unlimited access environment cannot easily constrain access by external intruders, but direct physical contact with the computer can

be prevented and the actions that can be performed via communication lines may be restricted in various ways.

b. Authorization Control

- Operational security is, to a large extent, concerned with the authorization process. The most critical aspects of this process relate to:

  - Who wishes to access or alter information?

  - Which information will be accessed or altered?

  - What operation (i.e., MODIFY) is to be performed on the information?

- These aspects should be analyzed in terms of the controls appropriate to and/or necessary for the individual firm's security goals. (A complete security system would likely include controls on when, from where, and why information is accessed or altered.)

- WHO. Identification and Verification. The verification process usually includes something that the user: (1) knows (e.g., a password), (2) carries (e.g., a badge), or (3) has a physical characteristic (e.g., a fingerprint).

  - In many organizations it is common to use surrogates such as an administrative assistant to obtain reports on behalf of the president. Considerable attention is warranted for both the technical mechanism for assigning roles, such as giving someone the "president's badge," and the procedural mechanisms for ensuring the correct and legitimate behavior of an individual acting as a surrogate for someone with more security authorization.

  - In many systems there is no way to distinguish among the multiple individuals that are allowed to take on a specific role (e.g., acting for

the president). Without such a differentiation procedure it is difficult to effectively audit such a system or to trace responsibility.

- WHICH. Classification of Information. The classification procedure can be complicated by many factors, such as granularity and security level.

  - Granularity denotes the level of detail of information to be classified, such as an entire document, a record, or a specific data item. A single document may contain a variety of information that may warrant separate classifications.

  - In certain types of computerized data bases the concepts of documents, or even records, may not explicitly exist. In such a situation it becomes necessary to authorize on the basis of specific data items or data types.

- The use of security levels is largely motivated by the military concept of security classifications, such as confidential, secret, and top secret.

  - Most nonmilitary organizations also use this concept to some extent (e.g., company confidential, company registered confidential, etc.).

  - Various combinations of information classification schemes could be employed in organizations.

  - Combining "horizontal" partitioning (i.e., functional) with a "vertical" partitioning (i.e., security level) is a common choice.

- WHAT. Operations upon Information. Once the "who" and the "which" have been established, it must be determined what actions are to be allowed.

  - As a simple example, one can distinguish between the operations "read" and "write."

- In the first case, an individual may be authorized to obtain certain information, such as a customer's bank balance, but have no authority to change it.

- In the latter case, authorization to change the information, such as changing the customer's bank balance, may be given.

- Variations of these two basic operations should be considered. For example, the actions of "creating" or "destroying" records are often treated differently from "reading" and "writing."

  - An inventory control clerk may be authorized to update the inventory balances, but only the engineering department personnel may be authorized to create new part records.

  - Other versions of "reading" can be used. For example, some systems allow access to statistical information (e.g., average salary) without providing access to the individual salary information.

  - Also, especially for proprietary software, there is the notion of "execute-only" access, where someone may be authorized to use the program but not allowed to modify or read the program (reading the program would allow it to be copied and thereby stolen).

c. Operational Constraints

- Many managers fail to recognize that security mechanisms may cause additional hardship or inconvenience for their users.

  - If such mechanisms are not easy to operate, it is likely that they will not be used effectively. This is important because for most users security is not their sole job function.

- For example, an inventory control clerk's primary responsibility is to maintain up-to-date information on the company's inventory. If the security mechanism requires extra time to update the inventory status, it will be at odds with the clerk's primary job function and implicitly encourage shortcuts that may compromise the security mechanism.

- When one is devising an authorization and security mechanism, it is important to consider the operational environment and pick an approach that is likely to be easy and convenient to use.

  - This decison may involve compromise between degree of security and ease of use.

d. Reliability and Recovery

- As the capabilities and cost effectiveness of information systems have increased, the systems have become closely integrated into the operation of many organizations.

  - This has, in turn, increased the concern for reliability and recovery.

- In some cases, reliability and recovery procedures are concordant with security procedures.

  - Reliability mechanisms often include additional tests for potential errors in either the hardware or software. Some of these tests may directly, or with minor extension, also be used to test for potential security violations.

  - Other reliability mechanisms produce redundancy and duplication.

- One way to safeguard the company's key files and provide for effective recovery is to make one or more copies. Thus, if the original is destroyed, a copy can be used. Unfortunately, these copies may increase the exposure to security violations.

- Since under normal operation the duplicates are not used, stolen or replaced copies may never be missed.

- In order to address this specific problem, many companies are adopting new procedures whereby both the original and copy are used in normal operations, such as on alternate days.

- In this way it is more likely that missing information will be detected. In additon, the reliability of the copies can be confirmed.

- In one organization a spot check of their "backup copies" revealed that 25% were not usable due either to errors during the copying operation or to deterioration during storage.

e. Transitional Impact

- At times of transition the system is extremely vulnerable to security violations, especially if the transition is from a manual to a computerized system.

- This vulnerability is caused by various factors, including: (1) most users are not used to the new system and are likely to be careless; (2) the system itself may not include all the "ultimately desired" security facilities and the facilities provided may not be fully tested; (3) the operational and technical problems that usually accompany a transition may act as significant diversions for concurrent security violations.

  - Security considerations must be carefully factored into the transition plan to minimize these vulnerablilites.

- Exhibit III-1 summarizes the salient points in this section.

2. ORGANIZATIONAL IMPACT

- Computer system security often requires or causes organizational changes. Some of these changes are desirable and are concordant with the security objectives.

  - Other impacts may be detrimental to the security objectives and possibly to the organization as a whole.

a. Security Awareness

- The degree of awareness of data security as an issue and the possibility of security threats vary widely.

  - Although awareness is increasing, it is likely that the situation has not changed significantly from that reported in one study where it was concluded that only a small proportion of computer users use security features. As one senior manager of a timesharing firm stated, "Some customers are concerned about security, some are not; but they are all naive."

  - Furthermore, although most systems provided various special security mechanisms, only a handful were actually used and those were used by the most sophisticated users. The majority of the users assumed that the computer system was secure and that they were adequately protected.

- The need for user education is an important aspect of improved and effective security procedures and enforcement.

EXHIBIT III-1

SUMMARY OF MANAGEMENT FACTORS

MANAGEMENT PROBLEM	SECURITY SOLUTION
• Operational Considerations	• Control Environment
- Operating Environment	• Authorize Control
- Authorization Control	• Establish Constraints
- Operational Constraints	• Institute Reliability and Recovery
- Reliability and Recovery Factors	• Reduce Transitional Impact

- Part of this increased education and awareness will come about as a result of external factors, such as: (1) press and media coverage; (2) increases in direct personal contact with computer systems as these systems become more pervasive in organizations; and (3) advances in security, in both technique and cost effectiveness, that will provide a more natural and easier use of modern systems.

- Organizations may also find it valuable to accelerate the awareness process by developing or sponsoring specific education activities.

b. Personnel Impact

- When extensive computer security is introduced into an organization, some personnel may react negatively because of difficulty in getting their work accomplished and/or a feeling of loss of power. The first problem was briefly discussed earlier.

- In a secure system, people can no longer have unlimited, unrestricted access to the entire system. Management must explicitly determine each individual's access rights.

  - To the extent that possession of information is a form of power, individuals may resist and resent any decrease in information access rights, even if the information is not necessary for the normal operation of the individual's job.

  - Restrictions or the elimination of "hands-on" computer access by most applications and systems programmers is often a serious blow to the programmers' egos.

- To a large extent, the security-related aspects of personnel selection and assignment are very similar in both the computer and noncomputer environments; thus, much of the existing literature on such subjects (e.g., embezzlement) is applicable.

c. Compounding the Problems

- Computerized systems have introduced several new problems.

  - A computerized system often allows for much more streamlined and efficient operation by eliminating many of the traditional steps. The loss of an intermediate step may also negate any existing internal check.

  - The operation of computerized systems introduces many new roles and procedures for which the concepts of division of responsibility are not well established from experience with prior manual systems.

    . Since computer programs, to a large extent, act as surrogates for what were traditionally manual steps, one individual may inherit the conflicting responsibilities of writing both operational and auditing programs.

  - Finally, the separation of responsibilities between computer programmers and operators can easily lead to conflicting company objectives.

    . For instance, whereas in some cases it would be advantageous to hire only opeators with no programming ability, the company's advancement opportunities may contrarily encourage operators to aspire to positions as programmers.

    . The correct balancing of these potentially conflicting objectives must be carefully studied.

    . Various additional procedures and checks and balances can be developed to lessen the potential exposure due to security violations by computer operators.

3. ECONOMIC CONSIDERATIONS

- Key issues that must be resolved in order to determine security economics include: (1) a determination of the value of information; (2) an assessment of likely threats to the information; and (3) a determination of the costs of available security mechanisms and their effectiveness.

a. Information Value

- It should seem obvious that the determination of the value of information is a crucial step in any security decison as well as in normal information management.

  - Unfortunately, the evaluation process remains very subjective. The process not only requires placing a value on information, but also consideration of the fact that the same information may be perceived to have different values by different groups of individuals.

  - At least three separate interest groups are involved:

    . Keeper - the organization that has and uses the information.

    . Source - the organization or individual that provided the information, or to whom the information pertains.

    . Intruder - an individual or organization that may wish the information.

  - The value of information depends further on its type. The following are general categories of information type.

- Critical operating information, such as this week's sales orders and production schedule, may have a very high value to the keeper, but considerably less value to its sources (i.e., the customers) or potential intruders.

- Personal information (e.g., an individual's census data or medical information in the employee personnel file) may have a much higher value to the source (i.e., the individual) than to either the keeper or intruder.

- Proprietary information, including marketing forecast data gathered by a company, may be much more valuable to an intruder, such as a competing company, than to either the sources (i.e., sample customers) or the keeper, who may have already finished analyzing the data.

- The value of a specific type of information may be perceived differently by different keepers (or different individuals or groups within the "keeper" organization), sources, and intruders.

b. Threat Evaluation

- In evaluating threats, one wants to know the economic impact (usually interpreted as a loss or expense to the keeper or source) should a particular operation be performed on certain information.

  - Threat operations can be divided into major categories, such as:

    - Interrupt - disrupt the normal processing of the information. Note that an interruption may be an important concern even though the information itself may not be affected in any way.

. Steal or disclose - read or copy information for use by either the intruder or a third party (e.g., publishing the psychiatric records of a competitor).

. Alter - change information, such as the intruder's bank balance. This is probably the most obvious threat to most people.

. Destroy - permanently destroy the information; for example, by erasing a magnetic tape.

- There are, of course, alternative categorizations of threats as well as additional factors that may be considered, such as whether the action was intentional (e.g., an intruder breaking in) or unintentional (e.g., someone lost the data).

  - Although the intentional threats are often of most concern, the unintentional may be more frequent and, possibly, have greater economic impact.

c. Risk Evaluation

- The threat assessment is intended to determine the value of a certain action upon information.

  - In order to develop a rational security plan it is necessary to assess the probability of each threat occurring.

    . A common objective of most risk assessment strategies proposed is to arrive at a quantitative statement of risk, such as a decision analysis calculation of the expected value of the loss for each threat.

- Numerous problems are encountered in attempting to perform such a risk assessment.

  . First, determining the precise monetary value of a threat may be very difficult.

  . Second, there is usually a reluctance to assign a monetary value to threats that have social impact, such as disclosure of confidential medical information.

  . Third, as noted earlier, different individuals and organizations may assign different values to a given threat.

- There is also considerable difficulty in determining the probability of a threat occurring. Computer threats are too diverse and recent to make it possible to attain much statistical information.

  - A threat assessment is, therefore, the most subjective aspect of the economics of computer security and thus each assessment would have to be calculated in its particular context.

d. Countermeasures

- For each risk usually one or more countermeasures are possible.

  - Countermeasures are intended to decrease the risk either by decreasing the probability of the threat occurring or by decreasing the impact of the threat should it occur.

  - The probability of losing information can be decreased by adding new procedures to monitor the use and location of the information.

- The impact of having lost information can be decreased either by having copies of the information available or by setting up procedures in advance that enable rapid and inexpensive reconstruction of the information.

- The two major considerations for each countermeasure are its effectiveness and its cost. This information can provide the basis for a rational economic security plan.

  - A countermeasure is economically reasonable if its effectiveness, in terms of decreased risk, exceeds it cost. The organization can establish maximum risk levels and then select one or more economically justified countermeasures, as necessary, to reduce the total risk to below the maximum risk levels.

  - Many of the same problems that prevent precise threat and risk assessment exist in determining countermeasures' effectiveness and cost. On the other hand, IBM has made efforts to enumerate countermeasures and, at least qualitatively, rate their effectiveness and cost.

- One final issue that is often studied in the context of threats by intruders is the cost of the threat.

  - In theory an economically rational intruder will not expend more to initiate a threat than the expected gain from that threat (e.g., one would not reasonably spend $5,000 to break into a vault that one believed contained only $10).

  - One of the significant objectives of a security countermeasure is to increase the costs to an intruder so as to raise the price above the value the intruder anticipates, and thereby reduce the risk.

- The intruder's costs include resources necessary, such as technology, expertise, time, and opportunity.

- In addition, penalty costs, such as the possibility of detection and the resulting economic, personal, and social penalties, represent a potential expense to the intruder.

- Therefore, countermeasures that are based on ex post facto detection rather than prevention of threats may be equally effective at reducing risk of an intruder threat.

- Exhibit III-2 is a summary of the salient points of this section.

4. SECURITY OBJECTIVES

- As part of a meaningful security plan it is necessary to consider the objectives to be accomplished and the specific organizational responsibilities necessary to carry out the plan.

  - It has been noted that security violations by authorized insiders far outnumber those by external intruders. Thus, a plan focusing only on the outside intruder may not provide much of an increase in security.

  - Unintentional mistakes by insiders may even be a comparatively important problem in many organizations.

a. Security Validation

- Techniques and procedures to validate the reasonableness and consistency of data are important in reducing the frequency of unintentional errors and in providing a means of detecting or preventing various forms of intentional security violations by either insiders or external intruders.

EXHIBIT III-2

SUMMARY OF ORGANIZATIONAL FACTORS

ORGANIZATIONAL PROBLEMS	SECURITY SOLUTIONS
• Need for Security	• Build Security Awareness
• Need for Personnel Planning	• Educate the People
• New Computer-Related Problems	- Carefully Assess Impact
• Economic Considerations	• Determine Cost/Benefits of:
	- Information
	- Threat Neutralization
	• Evaluate Risks
	- Implement Countermeasures

- Simple format and range checks are common to most, but not all, information systems.

  . A typical format check would be the verification that the zip code of an address is five digits long.

  . A range check would, for example, verify that an employee does not report working more than sixty hours per week.

- More complex consistency checks can be very valuable though they are less frequently used.

  - Salary range checks may be conditioned upon organizational position. For the president of the company a wage payment of $2,000 per week may not be unlikely, whereas it might be suspicious for a clerk to receive such a salary.

  - In the same manner, shipments being sent to an address different from the customer's address may be suspicious.

  - Such consistency checks are much more complex and time-consuming, both to construct and to execute, than simple range checks since the procedures require comparing several different sources of information to determine consistency within individual records.

  - Although the specific mechanisms for actually peforming validation and consistency checks are largely technical issues, a determination of the extent of validation and the specific rules and procedures to be followed requires careful managerial consideration.

b. Surveillance

- As noted earlier, computerized systems have often provided ways to streamline operations and greatly reduce the number of steps and amount of paperwork involved in various activities.

  - These systems can also greatly increase the difficulty in detecting security violations.

  - Using the computer's capabilities, special surveillance procedures can be incorporated into the system. There are at least two major forms: (1) audit log; and (2) monitoring.

    (i) Audit Log

- Basic to the concept of an audit log or audit trail is a permanent record of every significant action executed by the system.

  - In the days of quill pen journals and ledgers, one log record was made of every order placed and another if the order was cancelled (rather than merely discarding or erasing the order record). In principle, log records were accumulated and never changed.

- An audit log can be used for several important purposes.

  - Security violation detection.

    . As illustrated by the example above, an audit log can be used to help determine and diagnose certain security violations (e.g., there would be a permanent record of the order entry, order pickup, and order cancellation).

- Traditional auditing.

  . An audit log, at least in part, is essential to tracing transactions through the system as required in normal financial auditing procedures.

- Minor and massive recovery.

  . In an on-line system, an audit log of some type is essential to allow effective recovery from malfunctions caused by software or hardware during normal operations.

  . The periodic (typically nightly or weekly) backup tapes would not yet contain records of the transactions for the current day.

  . With an audit log it would be possible to reconstruct information that may have been destroyed or invalidated due to the malfunction.

  . In cases of minor transient malfunctions, such a recovery may be automated and accomplished in a few minutes or even seconds.

- Correction of errors.

  . In many systems, especially on-line systems, an error may be detected by the user immediately, such as accidently typing the wrong account number or incorrectly deleting a specific account.

  . The audit log can be helpful in reconstructing data that may have been incorrectly altered.

- Deterrence.

  . The mere existence of an audit log may be a deterrent to many security violations, especially by insiders.

  . Even if one knows how to circumvent a given system's security procedures and normal checks and balances, the fact that one's actions may be detected from the audit log can be a deterrent.

- The concept of an ex post facto security mechanism as a deterrent is often neglected in the design of many security procedures.

  - The important point to note is that the computer system is only one part of the security process.

  - Just as in the case of a "successful" bank robber, ex post facto pursuit and prosecution are important elements.

- A careful managerial study is necessary to determine what information should be captured in the audit log and how it should be organized for most effective use.

  - A definite plan of active examination is necessary if security violations are to be detected in a timely manner.

  - In many installations audit logs are generated and stored away, but never used. The audit logs should be used in both a systematic and nonsystematic manner.

  - In the former case, standard reports should be devised that could be used to detect unusual situations, such as an unusually large number of invalids or incorrect log-in attempts, exceptionally large orders from certain customers, etc.

- An intruder who has sufficient knowledge of the standard report procedures may find a way to violate systems security that does not appear on any of the standard security check reports. (The standard cliche in movie burglaries is for one of the robbers to say, "The guard makes his rounds every 30 minutes; that gives us 25 minutes to break into the safe.")

- Nonsystematic behavior can be accomplished by introducing an element of randomness into the examination, either by having the checking programs randomly select transactions for examination, or by providing on-line access to the audit log enabling security officers or management personnel to browse arbitrarily through the information.

(ii) Surveillance Monitoring

- Monitoring is a more active form of surveillance. While the system is in operation, various forms of information and statistics can be gathered and displayed on special monitoring terminals.

  - This type of facility can be used for a variety of security and non-security related purposes.

  - Security violation detection.

    . Information system monitoring facilities can be used in a manner similar to closed circuit television and intruder detector systems.

    . They may be used in a summary mode to note any unusual situations, such as an incorrect log-in attempt, numerous data input errors, or an exceptionally large order (or withdrawal), or in a viewing mode to monitor in detail the actions of one or more specific terminal users.

- Education.

  . Such monitoring facilities can be extremely instructive to both new and current managers.

  . By actually seeing the system in operation at both the summary and detail levels, one can gain considerable insight into the operation of the organization.

  . Many incorrectly preconceived notions can be corrected and new patterns of operation can be observed.

- System performance and utilization.

  . By being able to monitor the system, its designers can explore possible areas of improvement.

  . In one case, it was observed that the lengthy "English-like" interface to the information system, though very popular with the infrequent management users, required excessive typing for the full-time system users and was the cause of most data entry errors.

  . This problem had not been brought to the attention of the designers during the previous six months of system operation because the data entry activity was organizationally and physically quite removed from the system designers.

- Many of the other points noted about the audit log apply to the use of a monitoring facility.

- There are two additional points that must be made about surveillance facilities.

  - First, the audit log and monitoring capability introduces additional possibilities for security violations (e.g., stealing the audit log may be easier than stealing the data base itself). Thus, the security of these facilities must be carefully studied.

    . In some installations extensive precautions may be made to secure the computer facility and the operational data while the backup and audit tapes are stored unguarded in the basement.

  - Second, use of the audit and monitor facilities must itself be audit-logged.

    . Otherwise a dishonest security officer or someone who finds out how to gain access to these facilities may be able to use them to violate security and operate undetected.

- Needless to say, the various surveillance mechanisms and procedures described above have definite implications for the privacy of the system's users.

  - The monitoring facility, for example, could essentially allow a manager to "look over the shoulder" of any terminal user indefinitely without the employee being aware of this monitoring activity. In this regard, such facilities are similar to concealed closed circuit televisions.

  - Careful consideration should be given to their mode and purpose for use, as well as the extent of the knowledge about the existence of these systems that the company should allow.

c. Authorization Control

- The authorization process is an extremely important issue with numerous facets. Two specific issues will be discussed in this section: (1) authorization control and (2) rigidity of authorization.

- The access control rules to be enforced by the system can be essentially viewed as merely another type of information in the system, but this information and the ability to change it has sweeping implications.

  - A possible analogy is the safe that contains the combinations to all the other safes.

- Changing the access control rules (i.e., changes to authorizations) can be accomplished in various organizational ways. These methods can be divided into three major categories: centralized, hierarchical decentralized, and individual.

  - Centralized.

    . A single individual or organizational unit, such as the security officer or data base administrator, handles all authorizations.

  - Hierarchical decentralized.

    . The central authorization organization may delegate some or all of its authority to subordinate organizations.

    . Accounting files may be placed under the control of the head of accounting. Authority may then be further delegated (e.g., authorization control for certain accounting files may be assigned to different managers within the accounting organization).

  - In most implementations, the higher authorities in the authorization hierarchy retain the ability to revoke or override authorization decisions made by their subordinates.

- Individual.

  - In this situation no static authorization hierarchy exists. An individual may be allowed to create information (authorization to "create" may be controlled by either of the earlier two approaches), and the system would then recognize that individual as the "owner" of the information. The owner may authorize others to access the information, pass ownership to someone else, or establish co-ownership arrangements.

- Each of these authorization approaches has advantages and disadvantages, which has led some organizations to develop combinations or variations of these basic strategies to meet their organization's needs.

- The centralized approach, not surprisingly, is largely motivated by the military concept of "security officers."

  - With the increasing concern over the corporate "information resource" and the establishment of a data base administration function in many organizations, this approach has been adopted by some companies and may be viable in small or highly structured organizations.

  - However, in most large volatile or decentralized organizations, the rapidly evolving functions and information, especially for test cases and development activities, as well as personnel turnover and reassignment, can result in an extremely large number of security authorizations required every day.

- The centralized approach may not be desirable in organizations with a high volume of security authorization changes or where the organizational structure is too complex or decentralized to allow effective and intelligent centralized control over authorization changes.

- The hierarchical decentralized approach has been widely recommended in the literature and is basic to the security implementation on certain systems, such as the Honeywell Multics system.

  - This approach allows the security authorization control to be delegated to the groups that can most effectively administer and monitor these controls.

  - From an organizational point of view this may be very important. For example, if a division or function operates as a separate profit center with control over is own expenditures and plans, then that division probably should have security authorization control over its internal data.

- A major problem with most implementations of this approach lies in the authority of higher levels in the authorization hierarchy to revoke or override all authorization decisions.

  - This ability is usually viewed as necessary for organizational (i.e., "the boss is the boss") and operational (i.e., to correct mistakes in authorization assignments) reasons.

  - However, no "private" information can exist in this sytem. By analogy to the normal office environment, this would be equivalent to banning locked drawers in employees' desks (i.e., not accessible by superiors).

  - This issue of "corporate privacy" (as opposed to the more commonly accepted concept of "personal privacy") has been a major factor in the

reluctance of many groups within corporations to computerize their records.

- Few individuals do not view as private at least some information records or notes pertinent to their organizations that are presently kept in the privacy of their offices.

- This problem is likely to increase significantly among white-collar workers and management as advances in office automation greatly increases the scope and diversity of information stored in computerized information systems.

- The approach of individual authorization control is used in many simple systems.

  - A convenient implementation is to allow the creator of a file to designate "owner" and "user" passwords for the file. The owner password allows one to change either of the passwords; the user password allows one to access the file.

  - Various authorization objectives can be accomplished using such a system.

    . Private information can be kept private simply by not divulging either of the passwords. (Note: It is assumed that no standard way is provided for anyone, whether president of systems programmer, to find the passwords for any file.)

    . Access or ownership rights can be awarded by giving the passwords.

  - One drawback to the password strategy is that is is impossible to identify all the people who know the password or to revoke access selectively.

- Alternative strategies can be devised to accomplish the same results without using passwords in the manner noted above.

- One problem with the individual authorization approach though, regardless of the implementation, is the potential for situations where it becomes necessary to override the security mechanism (e.g., the individual dies, becomes ill, leaves the company).

  - In general, any security mechanism can be overcome, though some mechanisms, such as cryptographic encoding, may be very difficult to break, even by the system's designers.

  - If the mechanism is easy to break, the "privacy" assumed above will not exist; if it is very difficult to break, the organization may suffer if adverse circumstances occur.

d. Access Control

- Computer systems, lacking discretionary judgement, require a precise statement of access control rules to be enforced. This requires that very careful thought be given to the establishment of these rules and the specific authorizations assigned.

- Most existing security systems either do not provide any security override mechanism, or the override is in the form of a "panic" button that can be invoked by the security officer or computer operator to suspend all security enforcement.

  - This approach is very crude, awkward to use, and may expose the system to security violations while security enforcement is suspended.

- Three levels of access control may be defined. The normal "access is allowed" or "access is prohibited" can be augmented by "access may be allowed."

  - In environments where high ethical standards are the norm and/or ethical behavior is encouraged by particular constraints (e.g., ex post facto prosecution), certain users may be assigned "access may be allowed" permission to another user's private information.

  - The user would then be required to acknowledge that this access is deliberate and to provide a brief explanation of the reason.

  - The final decision as to the appropriateness of the access is deferred to human review at a later time.

- This type of flexible security enforcement is rare in current security systems.

  - Further development of these concepts and capabilities is essential in order to avoid the extremes of impairing effective use of the system or reverting to ad hoc emergency procedures all the time.

e. Security Responsibility

- As should be clear from the preceding discussions, effective security requires the cooperation and planning of many people in an organization.

  - Although certain aspects, such a awareness, require the active participation of almost everyone in the organization, most of the planning and decision-making issues are best resolved by a small number of people who should be responsible for security planning.

- The problem of responsibility is complicated by the fact that at least three types of issues can be identifed, each implying a potentially different type of organizational responsibility.

- These three issue types are:

  - Policy.

    . Policy issues regarding the use and types of security procedures require the active participation, formulation, and acceptance by top management personnel.

  - Operational.

    . Mapping the policy decisions into practice requires a detailed knowledge of the organization's information processing activities and the available security enforcement technologies.

    . This type of activity would require the skills normally found in the data base administration, systems programming, and computer operations functions.

  - Economic.

    . It has been noted that many security issues are essentially economic decisions involving uncertainty or incomplete information and risks.

    . The decision to use a certain security procedure which costs X dollars and provides a specific but unquantified degree of protection against certain types of potential security violations is very similar to the decision to expend funds on a project to develop a new product.

    . In this context, the role of "risk managers" (i.e., individuals experienced in making such subjective decisions) has been suggested in the literature.

- The concept of risk managers has been used in a very broad context to accommodate the perception that important elements of risk exist at the policy and operational levels as well as for economic decisions.

  - Some security experts have recommended to top management that ongoing risk analysis teams be formed that include: (1) EDP operations management; (2) department managers; (3) applications programmers; (4) systems programmers; (5) internal auditors; and (6) physical security personnel.

- The specific security roles and responsiblities may vary from organization to organization, but careful planning and defining of responsibilities are essential to effective and operationally viable information system security.

- Exhibit III-3 summarizes the important points of this section.

5. SECTION SUMMARY ON MANAGEMENT CONSIDERATIONS

- This chapter has identified and categorized the key management policy and procedure issues relevant to the attainment of effective computer security. Although social, legal, and technical factors may be relevant in certain cases, the primary factors in each issue identifed center on management decisons.

  - Mangement must carefully weigh the oprational, organizational, economic, and accountability implications of each of these decisions.

  - As our reliance upon computer-based information systems continues to increase and to propel us onward toward an even more comprehensive "information society," these issues will become increasingly critical.

EXHIBIT III-3

SUMMARY OF SECURITY FACTORS

SECURITY PROBLEMS	SECURITY SOLUTIONS
• Consider Objectives	• Develop and Implement Planning Strategies
• Security Validation	• Implement Checking Procedures and Routines
• Surveillance Issues	• Use Audit Logs and Monitoring Procedures
• Authorization Control	• Establish Access Control Rules
• Access Control	• Define Levels and Rigidity of Controls
• Policy Issues	• Get Everyone to Participate

IV TELECOMMUNICATIONS SECURITY

IV TELECOMMUNICATIONS SECURITY

A. TECHNOLOGY OVERVIEW

- The key to understanding the vulnerabilities of data base driven data communications systems is recognizing that you are dealing, in relative terms, with a large population of users, massive amounts of data, many communications links, and perhaps a vast arrary of functions. This translates into a large number of possible places where the security of the system and integrity of the data may be comprised for fraudulent purposes.

1. TERMINAL PROTECTION

- In remotely accessible computer systems, the terminals may be teletypewriters, keyboards/displays, minicomputers or intelligent terminals, remote job entry stations, automated teller machines, or any other type of terminal.

  - Because they are the machines through which data are entered and output is received and can be used to perpetuate computer fraud, their physical security deserves consideration.

- All types of terminals have at least one thing in common - the need to be protected against sabotage or unauthorized use.

- Although the principles for determining proper physical location and the procedures for restricting access are essentially the same as those that apply to the central computer facility, the problems are even more difficult.

- Isolated locations, inadequate supervison, and user access by more people all increase the likelihood of compromised security.

- Access to the terminals should be restricted whenever possible.

  - It is particularly important to restrict access to terminals that are used to access or update sensitive data files, data bases, and programs. Access to such terminals should be limited only to people authorized to use the terminals.

  - If certain terminals are designated for on-line program development only, they too should be secured against unauthorized use. It may be desirable to isolate such terminals in locked rooms to which only authorized users have keys.

- There are many control features that are, or may be, built into the terminal itself to enhance security. Only some of the more common features will be discussed here.

- The terminal may be equipped with a lock that, in the absence of the proper key, prevents the terminal from being used.

  - Keys are provided only to authorized users of the terminal.

  - There are two problems with this feature.

    . Keys may be lost, stolen, or duplicated, and locks may be picked or bypassed.

. If a key is lost or stolen, or is suspected to have been duplicated, it may be necessary to rekey the lock and issue new keys to authorized users.

- It may also be necessary to rekey the lock if a previously authorized user's authorization is removed or changed; requiring the return of the key in no way assures that the key was not duplicated prior to its return.

- With regard to picking or bypassing a terminal lock, many of the locks and installations can be readily defeated by an amateur locksmith.

  . If an important fraud prevention measure relies on terminal locks, it would be advisable to get the opinion of a master locksmith on the extent to which the locks are manipulation-resistant.

  . Also, note whether electrical contacts on the terminal lock could be easily bypassed with a jumper wire by opening the terminal cabinet or tilting the terminal on edge to expose its internal wiring.

• Terminals may be equipped with magnetic card or badge readers.

- A legitimate card or badge must be inserted into the reader in order to activate the terminal.

- The cards or badges are distributed to authorized users only. Such cards or badges, in addition to activating the terminal, often play a role in the identification and authentication of the user, as will be seen in the next section.

- The keyboard of the terminal may be locked by the computer system whenever it suspects that an unauthorized person is trying to access the system or an authorized user is trying to access, change, or enter information he is not authorized to access, change, or enter.

  - Thus, the person would be prevented from further breaching the security of the system at least until the terminal was unlocked by the appropriate security officer.

- A terminal may have its own identification by which it is able to positively identify itself to the computer system.

  - The security code for the terminal identification is generally hardwired (installed in the circuitry where it is protected against tampering) in the terminal. This feature is particularly important if the terminal is not in a secure location; if the terminal is used to access sensitive data files, data bases, or programs; or if the communications network uses public dial-up or switching equipment (anyone from anywhere can dial up the system).

  - The problem of postitively identifying terminals is that if a terminal should malfunction or break, another terminal cannot either replace it or be used in its place without a time delay.

- A terminal might be equipped with a mechanism for checking messages transmitted to it to be sure that the messages were routed properly before displaying or printing the information.

  - This mechanism goes hand in hand with the terminal identification feature. It is important in the same situations and has the same drawbacks.

- Terminals should have a facility by which the user can prevent information that is entered from being displayed or printed.

  - This facility may be either automatic or manual (a user is required to press a special key).

  - This facility is very important for user identification and authentication and will be discussed below.

- Terminals may be equipped with the capability of enciphering and deciphering cryptographic information.

  - This is a particularly important feature in a remotely accessible computer system that maintains sensitive information. This will be discussed later in this report.

2. USER AUTHENTICATION

- The computer system in a remotely accessible computer system environment must identify, in a positive manner, each user.

  - Establishing the identity of the user is usually a two-step process involving two fundamental notions:

    . Identification - the process by which the user identifies himself to the computer system.

    . Authentication - the process by which the user offers proof to the computer system that he is who he claims to be.

  - The user generally identifies himself to the computer system by entering his name, employee number, or account number, or by inserting a card or badge that contains his name, employee number, or

account number into a card or badge reader. This identification, however, is insufficient for the computer system to identify the user in a positive manner.

- The computer system must be reasonably satisfied that the user is who he claims to be; therefore, it must verify the authenticity of the identification.

- There are three general bases on which the identity of the user may be established and authenticated:

  - Something known by the user, such as his employee number, password, or secret code.

  - Somthing possessed by the user, such as an encoded card or badge, or a key.

  - Something about the user, such as his fingerprints or hand, his voice, or his signature.

- Let us examine each of these three bases and identify their strengths and weaknesses.

- The user may both identify himself and authenticate his identity by something he knows.

  - He typically identifies himself by his name, his employee number, or his account number.

  - He may authenticate his identity by something else that he knows. The methods that may be used to authenticate a user's identity include:

    . Reusable passwords.

- . Once-only codes.

- . Limited-use passwords.

- . Question-and-answer sequences.

- Reusable passwords.

  - The most commonly used method for authenticating the identity of a user is the password.

  - In consumer-oriented electronic funds transfer systems (EFTS) the password is referred to as a personal identification number (PIN) or code (PIC).

    - . The user enters his password after having identified himself to the system by entering his name, employee number, or account number.

    - . With EFTS, the PIN/PIC is usually entered after the user has identified himself by supplying an encoded plastic card.

  - The disadvantage of a password is that something known by an authorized user of the computer system may become known to another person who is not authorized to use the system.

    - . That other person may then be able to impersonate the authorized user and, thus, be able to perpetrate fraud.

- There are several ways to minimize this risk and the resulting exposure:

  - The importance of keeping the password secret and secure should be impressed upon all users.

    . They should be told not to leave their passwords lying around where they can be observed by others. In fact, they should be discouraged from writing them down.

    . They should be encouraged to destroy any paper containing the password in such a way that another person cannot learn the password by retrieving the paper from the trash.

    . They should be encouraged not to divulge their password to anyone.

  - The password should be sufficiently short so that it can be memorized.

    . Passwords are generally four to eight alphanumeric characters. As mentioned above, it should not have to be written down to be remembered.

    . Perpetrators of fraud know the obvious and no-so-obvious places where passwords are recorded, such as on paper in a desk drawer or in a wallet, on a desk calendar, on tape stuck underneath the desk or terminal or on the desk drawer, or scratched onto the terminal.

    . On the other hand, the password must not be too short.

    . The degree of security of the password is a function of the possible number of combinations from which it is chosen. For example, if the password is two numeric characters, there are

100 possible combinations. If it is two alphanumeric characters, there are 1,296 possible combinations. If it is four alphanumeric characters and all possible combinations are used (i.e., the password does not have to be pronounceable or a valid English word), there are 456,976 possible combinations. If it is four alphanumeric characters, there are 1,679,616 possible combinations.

. The more possible combinations, the more difficult it would be for a perpetrator to guess the right one.

- The password should be fairly random.

. It should not be something that can be determined easily, such as a person's name or nickname, the name of an immediate family member, a person's birthdate, or the city in which the person resides.

- The password should be unique for each user.

. This serves two very important purposes. It reduces the likelihood that the password will become known to other people who are not authorized to use the system or to use that particular password. And, it fixes responsibility on the user if his password is used by an unauthorized person.

. This would discourage a user from allowing another to use his password because he, the user, would be held accountable.

- The password should not be printed or displayed when entered into the terminal.

  - If it is not possible to suppress the printing or display, the password should be concealed by over- or under-printed characters.

  - Embedding special nonprinting characters in the password will also help to conceal the password.

  - Concealing the password when it is entered will make it difficult for a perpetrator to secretly observe the password as it is entered.

- The password should never be printed on output reports.

- The password should be changed periodically and whenever a compromise of the password is suspected. This will minimize the exposure resulting from the compromise of a password.

- In timesharing systems, users generally change their own passwords. In data base systems, it is more common to find that the passwords are changed centrally for all users at the same time.

- Although this ensures that the passwords are changed, it introduces an additional risk of compromise because the new passwords must be distributed to the users. The risk can be minimized.

  - If the users know what day the new passwords are being distributed, they can be instructed to notify the appropriate person if they do not receive the new password, or if the transmittal (i.e., envelope or mailer) appears to have been tampered with or opened.

  - They can also be required to positively acknowledge receipt of the password by signing and returning a turnaround document accompanying the password.

- What should the system do if a user enters an incorrect password? Realizing that everyone makes mistakes, the system should give the user a second chance.

  - If the second entry is also incorrect, the system might:

    . Give the user one last chance to enter the correct password.

    . Lock the terminal keyboard in such a way that it can only be unlocked by an appropriately authorized individual.

    . Refuse to give the user another chance for a period of time, such as one minute. This will thwart any schemes to guess a password that are based on high-speed trial and error.

    . Keep the user trying and prevent him from accessing any sensitive data and from performing any unauthorized activities if he should guess the password, while alerting the appropriate security officer at the particular terminal location to the attempted penetration of the system. In this way, the perpetrator may be caught redhanded.

  - Regardless of the action taken by the system, the system should, at a minimum, inform the person at the central security control location (the computer security officer) of the attempted penetration.

- We have already identified several ways that a perpertrator might learn an authorized user's password.

  - Finding it written down.

  - Finding it printed on terminal paper or output reports.

- Observing the user entering it.

- Intercepting the distribution of new passwords.

- Guessing it.

- Being told what it is by the user.

- For a really determined perpetrator, there are other ways as well:

  - The perpetrator might learn it by tapping the communications lines.

  - The perpetrator might learn it by penetrating the operating system and accessing the file of passwords.

  - The perpetrator might use a piggyback penetration scheme.

    . He might insert a minicomputer into the communications lines and intercept the user's sign-on.

    . The minicomputer would return the expected system responses to the user until the user enters his password.

    . Then the minicomputer would respond with an innocuous message (i.e., that the system has failed) and would disconnect the user.

  - These last three exposures may be controlled by encrypting the password during transmission and by encrypting the file of passwords. The subject of decryption will be discussed later.

- Once-only codes can also be used to protect the system. These are essentially passwords; however, they become invalid as soon as they are used once. Thus, if they are observed being entered, they cannot be used again.

  - Once-only code schemes are implemented in one of two ways.

    . A user may be issued a new code or password whenever he uses the one that he has.

    . Alternatively, a user may be supplied with a list of passwords that must be used in succession.

  - The user must be instructed not to mark off the passwords as they are used so that it will not be apparent which password is to be used next.

- There are advantages and disadvantages to using once-only codes.

  - The advantage of single once-only codes is that they do not have to be written down.

  - The disadvantage is that they are vulnerable to exposure during distribution.

  - In addition, in an environment in which the system is accessed frequently by users, the need to get a new code before each access is time-consuming and cumbersome.

- The advantages of lists of once-only codes are that the risk of exposure during distribution and the time involved in distribution are significantly decreased.

  - The disadvantage is that the codes are written down.

- Unless the user keeps the list secure, it may fall into the hands of a perpetrator. Even if a user has not marked off the codes he has used, the perpetrator has only a finite number of passwords from which to choose.

- The odds of guessing the proper code are significantly increased, especially if the system gives him three chances to enter the correct code.

- It may be desirable to invalidate the current list as soon as one incorrect password is entered and to issue a new list. Although this will prevent trial-and-error schemes, it does not take into account the fact that an authorized user is bound to make a mistake entering the code at one time or another.

- Limited-use passwords. The advantage of reusable passwords and once-only codes may be combined by associating expiration dates or maximum number of uses with a password. For example, the password may expire on the tenth day of the following month. Or, the password may expire after it has been used 17 times. The password can be memorized; it need not be written down.

  - The password must be changed periodically, thereby limiting the amount of exposure if the password should be compromised.

  - Moreover, if a usage count is implemented or if expiration dates are staggered, new passwords are not distributed to all users at the same time.

  - This may serve to reduce the risk of exposure during distribution because a perpetrator might not be able to find out the distribution date.

- Question-and-answer sequences. Question-and-answer sequences are another method to authenticate the identity of a user.

- This method does not use passwords or codes at all.

- The user is asked a series of personal questions to which only he presumably knows the correct answers. The questions may pertain to the user's family (e.g., names, birthdates, birthplaces, anniversaries, etc.), to the user's background (e.g., former addresses, schools attended, teacher's names, etc.), to the user's interests and hobbies, or to the user's preferences (e.g., favorite color, favorite food, etc.).

- The disadvantage of question-and-answer sequences is that they significantly slow down the sign-on procedure and may become very tedious to the frequent user.

- It is desirable to maintain a file of questions and then to randomly select a few questions to ask during a particular sign-on.

- The number of questions asked depends upon several factors, including the time involved in signing onto the system, the number of possible answers to the questions, and the ease with which a perpetrator may successfully guess the answers.

- Yes/no and either/or questions are much easier to guess than such questions as "What elementary school did you attend?" or "Where (in what city) was your mother born?"

- The benefit of asking different sets of questions at each sign-on is that it would be difficult for a perpetrator to learn the correct answers by observing one, or even a few, sign-on sessions.

- Because the question-and-answer technique relies on factual information that is somewhat likely to be known by others (friends, coworkers, people with access to personnel and credit records, dossiers, etc.), it should not be used as

a sole basis for authentication and should be avoided in high-security applications.

3. USER IDENTIFICATION

- The user may be given an encoded card or badge, a key, or some other physical item by which to identify himself or to authenticate his identity.

  - Typically such items are used to establish the identity of a user, and a password, code, or PIN is used for authentication of the identity.

- Encoded cards or badges are particularly appropriate in situations where several users share a terminal.

  - Each user is supplied with his own card or badge. The terminal is equipped with a reading station into which the card or badge is inserted.

  - Some terminals may be designed to accept only specific cards or badges. Such terminals, thus, have internal lists of the authorized cards or badges; the lists may be changed by the security officer as authorized users change.

  - Other terminals simply read the card or badge and the computer system establishes the identity of the user.

- Keys are appropriate when a single user is assigned exclusive use of a terminal for a fixed period of time.

- The disadvantage of cards, badges, and keys is that they may be lost, stolen, or duplicated. They may even be stolen, duplicated, and returned without leaving a trace.

- Keys and locks have an additional disadvantage; locks may be picked.

- If a card or badge is lost or suspected to have been duplicated, a new card or badge must be issued and the list of authorized cards or badges must be changed to reflect the change of cards.

- If a key is lost, stolen, or suspected to have been duplicated, a new key must be issued and the lock must be rekeyed.

- If there is a change in authorized users, and cards or badges are used, only the list of authorized cards or badges need be changed.

  - However, if keys are used, the lock may have to be rekeyed.

- Optically encoded cards may be the least secure of all physical items because the coding is visible. Magnetically encoded cards may be the most secure because they are the most difficult to duplicate.

- Developmental efforts are currently focused on perfecting ways to authenticate the identity of a user by the user's personal and behavorial characteristics.

  - It should be noted that personal and behavioral characteristics are not used to establish the identity of a user. They are used only for authentication.

  - The characteristics receiving the most attention are:

    . Fingerprints, including pattern and other distinctive marking recognition factors.

    . Hands, including the shape or translucency of the hand, the length of the fingers, and the curvature of the fingertips.

. Signature patterns.

. Signature analysis, including the velocity, acceleration, and pressure characteristics exhibited whenever a person signs his name.

. Voice recognition.

- The key considerations with regard to the effectiveness of these characteristics for identification validation are their ability to be copied or forged, the ability of a perpetrator to obtain and enter a copy of an authorized person's characteristics (i.e., a copy of the signature), and the degree of interpersonal and intrapersonal variations of each characteristic.

- Interpersonal variations are the variations of a particular characteristic from one individual to another.

- Intrapersonal variations are the variations of a particular characteristic exhibited by one individual.

  - A person's voice or signature may be affected by several factors, including his health, his emotional condition, his physical condition, or stress.

  - A person's fingerprints or hand may be affected by injuries.

  - The degree of intrapersonal variations necessitates the incorporation of tolerances into the recognition process.

  - As the tolerances are increased, the chances of one individual impersonating another also increase.

- Thus, the probability of a perpetrator successfully gaining access to the system is increased.

4. AUTHORIZATION

- Modern computer systems have innumerable advantages over their predecessors, one of which is the ability of users to share data and programs.

  - This sharing must be controlled if the integrity and confidentiality of the data and programs are to be preserved.

  - Permission must be granted to authorized users of the system and to production programs to access the data and programs and to perform some functions (such as execute, read, copy, write, or modify) or combinations of functions.

- This permission is commonly referred to as authorization.

  - Authorization is granted by user management to specific users or groups of users.

  - Authorization must be implemented or enforced by the security software of the computer system.

- There are several methods for specifying and implementing authorization. Regardless of the approach employed, several principles should be established to ensure that the approach is effective in controlling unauthorized or fraudulent actions.

a. Authorization Principles

- Authorization should not be confused with user identification and authentication.

- User identification and authentication is the procedure by which the user establishes and authenticates his identity and the computer system determines whether or not he is a legitimate user of the computer system.

- Authorization is performed after user identification and authentication. It is the procedure by which the computer system determines whether the user has been given the explicit right (has been authorized) to perform certain actions, such as entering specific types of transactions; executing, reading, or modifying specific programs; or, reading, modifying, or copying specific data.

- Authorization is also the procedure by which the computer system determines whether or not particular production programs and system software programs have been authorized to access other production or system programs and data.

- The system must be able to determine whether the user's, or the program's, actions are authorized. Thus, some mechanism for identifying the actions that a user or program is authorized to perform must be established and implemented.

- Each and every access to every data file, data base, program, or component thereof should be checked for proper authorization.

  - The security system, whether it is part of the operating system, part of the data base management system, or an independent system, must determine whether or not each access is authorized.

  - Furthermore, it must determine whether the functions to be performed are authorized.

- It is not enough to determine the authorization upon the first access only. A perpetrator's strategy may be to try to hide unauthorized actions among authorized and benign actions.

- The security system must be able to enforce the authorization rules not only in static, unchanging environments, but in dynamic environments where authorizations may change quickly and frequently as well.

  - It must not be possible to confuse the security system (e.g., by chaining so many calls to the security that it ceases to function properly), thereby causing it to lose control, if the system is to be effective.

  - Systems that can be confused and penetrated in dynamic environments have been exploited by perpetrators of fraud. If the security system can be penetrated, the system and all its resources (data and programs) may be completely vulnerable to exposure, compromise, unauthorized modification, and possibly destruction.

  - Even if the environment is static, situations may arise that require changes to authorizations to be effected quickly.

  - Such a situation might arise if any employee is suspected of perpetrating fraud, or if an employee is suddenly terminated or transferred. The system must be able to accommodate such changes.

- Every user and program should use only those resources that are needed to do the particular job at hand.

  - Just because a user or program may be authorized to access several system resources (system software, production or test programs, data) and to perform several functions (read, write, modify, execute) on those resources, he, or it, should not invoke all the authorizations if only one or two particular authorizations are necessary at the time.

- Only those portions of the system that must be exposed should be exposed.

- The default condition must always be a denial of access.

  - Unless a user, terminal, or program has explicit authorization to enter a particular type of transaction or to access a particular data file, data base, program, or component thereof and perform the requested function on the item, the requested transaction or the access and the function must be denied.

  - The user must also be denied any instructions or prompts that relate to the requested action.

  - Some computer systems tend to view users, terminals, and programs as benign and to permit access to system resources even if the user, terminal, or program was not explicitly authorized. This is not an acceptable method of operation. It exposes your data and programs to disclosure, compromise, unauthorized or fraudulent modification, and destruction.

- Users' actions must be monitored and users must be held accountable for their actions.

  - Users must know that they will be held accountable for all unauthorized actions performed either by them or in their name (using their identification and authorization).

  - Knowing that there is a high probability that they will be caught if they do anything unauthorized or if they allow something unauthorized to be done in their name is an effective deterrent to fraud.

- Regardless of the approach used to implement authorizations, it is of utmost importance that the tables or files containing the authorizations be tightly secured against browsing (reading through the tables or files) and modification by anyone other than the computer security officer.

  - It is also critically important that all changes of authorizations be carefully reviewed and monitored by management.

b. Authorization Specification

- The specification of authorizations involves three elements:

  - Resources (protected objects).

  - Functions (actions/operations).

  - Subjects (system users).

- These three elements must be specified regardless of the approach used to implement authorization.

- Resources.

  - The resources, or protected objects, are the types of transactions, the data, and the programs available in your computers system.

  - Authorization may be granted at one or more of the following levels:

    . Entire data file, data base, or program.

    . Particular group items within the data base.

- Particular records or categories of records within the data base or data file.

- Particular data fields or categories of data fields within the data base or data file.

- Particular bits within the data fields of a data base or data file.

- Particular data fields or records within the data base or data file, depending upon the value of the particular data field or of another data field.

- Particular data fields or records within the data base or data file, depending upon the number of records or fields that meet the selection criteria.

- Particular transactions or types of transactions.

- A user may be authorized to access the entire data file or data base, or he may be authorized to access only particular components of the data file or data base.

  - This access to particular components of the data file or data base may be dependent upon the value of the particular component or the value of some other component.

    - For example, a user may be able to access the entire payroll file or data base, or only the payroll records of all employees in his department.

    - Or, he may be able to access the payroll records of employees in his department whose annual salary is less than $20,000.

. Or, he may be able to access the payroll records of employees in his department whose annual salary is less than $20,000 only if there are at least five employees in that category.

- Functions.

  - Whereas access to the protected objects may be granted at one or more of the above-mentioned levels, the functions that the user or subject may be authorized to perform may be restricted.

  - The user, program, or terminal may be authorized to perform one or more of the following functions on the protected objects.

    . Read.

    . Execute.

    . Update (add or delete particular records or fields).

    . Modify (change particular records or fields).

    . Print or copy.

    . Enter (input particular transaction types).

- The authorization for performing these functions may also be dependent upon the time of day, the time or day during an accounting period, the terminal used, the values of particular data fields, or the number of records or fields that meet the selection criteria.

- Subjects.

  - The subjects are the users, the programs, and the terminals used. The subjects are the initiators of the request to perform a specific function on specified protected objects.

  - The subjects may be:

    . Individual users.

    . Categories or groups of users.

    . Individual terminals or groups of terminals (i.e., location).

    . Individual programs (system software and production).

    . Categories of programs (system software and production).

c. Authorization Implementation

- The relationship among the protected objects, functions, and subjects must, in some way, be made available to the computer security system.

  - There are numerous ways to implement authorizations. This section will now examine a few of the more common ones:

    . Data and program stratification.

    . User compartmentalization.

    . User security profiles.

    . User security codes.

- Terminal security codes.
- Transaction authorization tables.
- Record-type authorization tables.
- User/record-type authorization tables.
- Passwords.
- Access control lists.

- It is important to remember that as authorizations become more detailed and refined, the authorization mechanisms become increasingly complex.
  - Several involved calculations may be necessary to implement authorizations based upon particular data values or upon numbers of items meeting selection criteria.

- Data and program stratification.
  - The data and programs may be stratified, or classified, by the degree of security to be provided to them.
  - All data and programs of a confidential and extremely sensitive nature might be in one class.
  - Another class might contain confidential data and programs. The number of strata, or classes, defined is dependent upon the number of security levels defined for the data programs.
  - This stratification may be carried over into computer memory.

- The hardware implementation of stratification is referred to as "rings of protection." Memory is divided into segments. Each segment is assigned to one, and only one, ring.

- Thus, hardware isolation may be provided to the various strata of data and programs.

- User compartmentalization.

  - Users may be compartmentalized or grouped according to the access privileges afforded to them. The compartments may contain one user identification, or hundreds. The number of compartments or groups defined depends upon the variety of access privileges that are permitted for individual users.

  - All users of a given group have the same access privileges.

  - Compartmentalization has also been used to define organizational groupings.

    - Each compartment thus contains the user identification for all users in one department or in one area within a department.

    - Each compartment would then be stratified according to the various levels of access privileges of the users in the group.

  - As with stratification, compartmentalization may have a hardware isolation couterpart which involves subdividing memory into sections with different access privileges.

- User security profiles.

  - A security profile may be established for each user. It typically contains user identification information, including employee number, department number, and the user's access privileges.

  - In systems employing compartmentalization, the profile might or might not contain the user's access privileges. It would, however, indicate the compartment of which he is a member.

- User security codes.

  - Users may be assigned security codes. The access privileges might then be defined in terms of the security codes.

  - If each user is assigned one security code, the code might be defined in his profile.

  - The user might also be required to enter his security code during sign-ons as an additonal identification authentication mechanism.

  - Alternatively, users may be assigned two or more security codes, depending upon the types of work they are to perform.

    . The security code entered during sign-on would have to be validated to ensure that the user is authorized to use that code.

    . This multiple-security code concept is a variation of compartmentalization in which users may belong to multiple groups.

    . The user authorization tables might use the security codes as the subjects.

- Terminal security codes.

  - Terminals might also be assigned security codes. The terminals' security codes are generally defined in terminal profile tables or files.

  - Security codes for a particular terminal might be used to:

    . Define the types of transactions and types of actions that can be performed using that terminal.

    . Define the users authorized to use that terminal.

    . Define the types of information that may be sent to that terminal.

  - The terminal security code might serve as a limiting factor in the sense that if the user's authorization is greater than the terminal's, the user may be limited to using the terminal's authorization rather than his own.

- Exhibit IV-1 depicts a user sign-on in which the user is assigned a once-only security code. The terminal identification is used to identify the terminal and identify the users authorized to use the terminal.

- Transaction authorization tables.

  - Authorization tables define the relationships between subjects, protected objects, and functions. A simple transaction authorization table is depicted in Exhibit IV-2.

  - The subjects are the users, identified by their user identification numbers. The protected objects are the available types of transactions. The functions are represented by a single bit: 0 (entry is not

EXHIBIT IV-1

FLOW DIAGRAM OF SIGN-ON VERIFICATION

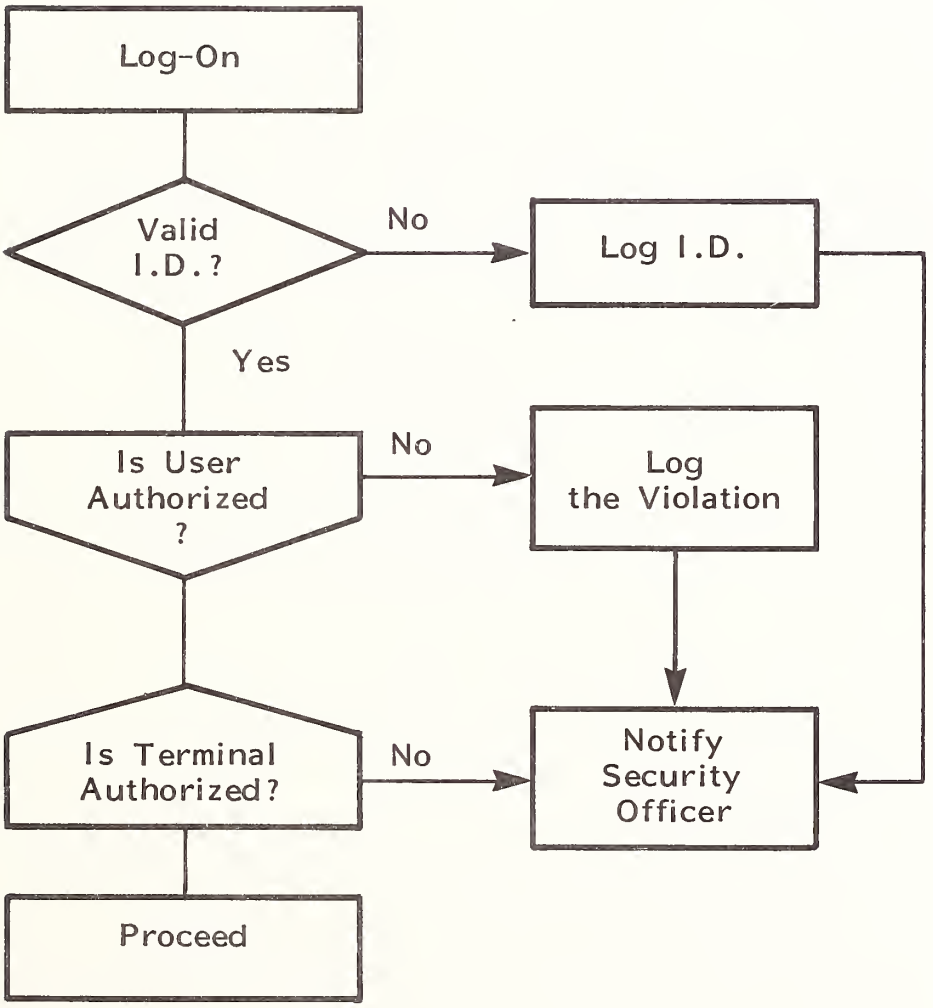


EXHIBIT IV-2

EXAMPLE OF USER AUTHORIZATION TABLE

USER I.D. (EMP. #)	TRANSACTION TYPE				
	1	2	3	4	5
21705	0	0	1		
21710	1	1	1		

Bit 0 = Not Authorized

Bit 1 = Authorized

authorized) and 1 (entry is authorized). Thus, there is one entry for each user, specifying whether or not the user is authorized to enter the particular type of transaction.

- Record-type authorization tables.

  - Another type of authorization table is depicted in Exhibit IV-3.

  - In this table, the subjects are the individual users who are identified by their employee numbers.

  - The protected objects are the various types of records. Three bits are used to specify the functions that the particular user is authorized to perform on the specific type of record.

    . The first bit indicates whether he is authorized to read the particular type of record.

    . The second bit indicates whether he is authorized to modify the particular type of record.

    . The third bit indicates whether he is capable of modifying the particular type of record.

    . He may be authorized to modify the particular type of record as a function of his position in the organization. However, he may not be capable of modifying the particular type of record until he has received additonal training, has spent a minimum amount of time in the position, or has gained more experience.

EXHIBIT IV-3

EXAMPLE OF DATA RECORD AUTHORIZATION TABLE

USER I.D. (EMP. #)	RECORD TYPE A			RECORD TYPE B			RECORD TYPE C		
	R	A	N	R	A	N	R	A	N
21705	1	0	0	1	1	1	0	0	0
21710	1	1	1	1	1	1	1	1	0

R = Read

A = Authorized to Modify

N = Not Authorized to Modify

- User/record-type authorization tables.

  - We have looked at two relatively simple authorization tables. Let's now take a look at a more complex authorization table.

  - Implementation of authorization may, in some cases, be best handled by setting up multiple authorization tables. One such approach is depicted in Exhibit IV-4.

  - In this exhibit there are two authorization tables: one for the user and one for the data.

  - The user authorization table is essentially a user security profile. It contains one entry for each user and defines each user's security code, the group of terminals each user is authorized to use, and the user group or compartment of which each user is a member.

    . The computer security system may be able to verify that the user is authorized to use a particular security code and to use a particular group of terminals.

    . It can determine the user's compartment or group from the user authorization table.

  - The subjects in the data authorization table are the user groups instead of the individual uses.

    . The protected objects are the various categories of records, referred to in the exhibit as "data groups."

    . Each user group's authorization with respect to each record category or data group is represented by two bits: 00, no permission; 01, permission to read only; 10, permission to read

EXHIBIT IV-4

MULTIPLE AUTHORIZATION TABLES

User Authorization Table

User Number	Security Number	Terminal Group	User Group
U_1	S_1	T_1	G_1
U_2	S_2	T_2	G_2
U_3	S_3	T_3	G_3

U = User Number
S = Security Number
T = Terminal Group Number
G = User Group Number
D = Data Group Number
A = Type of Authorization (2 bits)
- A_0 = No Permission
- A_1 = Permission to Read Record
- A_2 = Permission to Read and Update Record
- A_3 = Permission to Read, Update, Create or Delete Record

Data Authorization Table

User Group	Data Groups															
	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8	D_9		D_{396}	D_{397}	D_{398}	D_{399}	D_{400}
G_1	A_1	A_0	A_0	A_3	A_0	A_0	A_1	A_0	A_1						
G_2	A_0	A_0	A_1	A_1	A_0	A_0	A_1	A_0	A_2						
G_3	A_0	A_2	A_0	A_0	A_0	A_1	A_0	A_0	A_0						
G_4	A_0	A_0	A_3	A_3	A_1	A_0	A_0	A_0	A_0						
G_5	A_0	A_0	A_1	A_1	A_0	A_0	A_0	A_0	A_0						
G_6	A_0	A_2	A_1												

Alternative Layout

Data Authorization Table

User Group	Data Groups and Authorization										
G_1	D_3A_1	D_5A_2	$D_{31}A_1$	$D_{72}A_2$	$D_{100}A_1$		$D_{207}A_1$	$D_{211}A_3$	$D_{398}A_1$	$D_{399}A_2$	$D_{400}A_2$
G_2	D_3A_1	D_5A_1	D_7A_1	$D_{66}A_1$	$D_{71}A_1$						
G_3	D_3A_2	D_5A_1									
G_4	D_3A_2	D_4A_3	D_5A_1	$D_{38}A$	$D_{399}A_2$						
G_5	D_3A	D_4A_1	$D_{20}A_2$	$D_{21}A_1$	$D_{22}A$						
G_6	D_2A_2	D_3A_1	D_6A_1	D_7A_1							

and modify; 11, permission to read, modify, and create or delete records.

. Each time the user requests a particular record, the system must determine the user's user group from the user authorization table.

. It must then determine the user group's authorization with respect to the particular type of record in the data authorization table.

- The alternative layout for the data authorization table represents the situation in which each user group is only authorized to access a small subset of the available record types.

. Each entry identifies the protected object, record type that the user group may access, and the functions that may be performed on the particular record type.

- Passwords.

- Program and data files may be password protected.

- A user or a program wishing to access a particular file might have to supply the proper password. Files may be protected by multiple passwords.

- Each password may have access privileges associated with it; therefore, the password supplied by the user or the program might define the functions that can be performed on the file.

- Users and programs would be given only the password that corresponded to the privileges afforded to them.

- The disadvantage of the password protection is that the passwords must be communicated to the authorized users. They are thus vulnerable to exposure during distribution.

  . Each user might be given a unique password rather than giving users with the same access privileges the same password.

  . This provides more security because each user can be held accountable for actions performed using his password. Users would, therefore, be less likely to divulge their passwords to others.

- Access control lists.

  - Files may be labeled with lists of users authorized to access them and their access privileges. Each time a user tries to access a file, the access control list for the particular file is scanned to determine if the user is authorized to access the file and if he is authorized to perform the function he is requesting.

  - Files may be segmented and each segment may have its own access control list. Access control lists may be used in conjunction with user compartmentalization, security profiles, and password protection.

5. SURVEILLANCE

- Methods for detecting possible security violations must be implemented in communications and data base systems.

  - Effective methods of detecting security violations will deter many people who are considering violating the security of a system and its data because there is a good probability that they will be caught.

- In addition to acting as a deterrent, effective detection will make it possible to identify some of the weaknesses in the security system. Such weaknesses can then be corrected.

- There are basically two types of surveillance.

  . Realtime surveillance in which immediate action may be taken.

  . Logging or after-the-fact surveillance.

- The following checks can be made in realtime:

  . Invalid user identification.

  . Invalid user identification authentication.

  . Invalid security code, or security code inconsistent with user identification if the user supplies his security code.

  . Unauthorized terminal identification.

  . Authorized terminal used by unauthorized user.

  . Unauthorized request to process, read, or modify programs or data.

  . Unauthorized transaction type entered (unauthorized user and/or unauthorized terminal).

  . Maximum number of invalid or incorrect entries made or actions taken.

- As discussed earlier, when suspicious situations are detected it may be necessary, or desirable, to take immediate defensive action.

  - In other situations, recognizing that everyone occasionally makes mistakes, it may be desirable to give the person a second chance and possibly a third before taking action.

  - For instance, depending upon the method of authentication used, you might want to give the user three chances to enter his password correctly before taking action.

  - On the other hand, you might want to take action as soon as two unauthorized data access attempts have been made in a row or during a given terminal session.

  - Regardless of the situation, all such errors and violations, including the first, should be logged.

- One type of surveillance that may be categorized as a realtime check involves the printing of the password or authentication usage count on the terminal after user identification and authentication have been completed.

  - The user might know that the last time he entered his password the usage count was, say, 17. If it is now 19 or 20, he should suspect that someone had used his password and should immediately notify the local and the central security officers.

- Automatic teller machines, used in an Electronic Funds Transfer (EFT) environment, frequently issue transaction receipts that contain a transaction count or countdown (i.e., number of uses remaining) if a limit is placed on the number of times the machine may be used with a particular magnetically encoded card.

- A similar type of surveillance check would be if a single once-only code was rejected or if the next sequential once-only code on a list was rejected.

  - Regardless of the exact nature of the situation, any time an authorized user is unable to complete his identification and authentication, he should immediately notify the local and central security officers.

- Logging is every bit as important as realtime surveillance because logs make it possible to identify patterns of attempted security violations and weaknesses in the security system.

  - They also provide an audit trail in the event that an unauthorized activity occurs that was not detected by the security system.

- Some of the more important logs that should be produced by the system include:

  - All attempts, both valid and invalid, to access the system should be logged.

    . The following information should be recorded: date, time of day, terminal identification, user identification, and an indication of whether the attempt was valid or invalid.

    . If the attempt was valid, the nature of the access and the sign-off time should also be recorded.

  - This log provides an audit trail which may prove invaluable in investigating unauthorized activity that is detected after it has occurred.

    . For example, suppose a master file record had been changed improperly.

- One log might identify dates and times the master file was updated.

- Using information from this log and the terminal audit trail, it may be possible to pinpoint the user identification (user ID) and the terminal used to perform the unauthorized change.

- The log will also help to identify vulnerable user IDs, vulnerable terminals, and the vulnerable times of day. Invalid access attempts for a particular user ID may indicate that the user's identification and authentication were partially compromised.

  - The user may have lost his card, badge, or key; or his card, badge, or key may have been stolen, duplicated, and returned without his knowledge.

  - The user's list of once-only codes may have been compromised.

  - The log will identify the user ID with a problem.

  - The action to be taken depends upon the nature of the problem. It may involve issuing a new card, badge, key, single once-only code, or list of once-only codes, and invalidating the current one. It may involve providing additional training to the user in the use and security of his identification and authentication.

- If a particular terminal is the subject of frequent or numerous invalid access attempts, it may be necessary to strengthen the physical security of the terminal.

  - If there are particular times of day when many, or more, invalid access attempts occur, the conditions at that time of day should be studied and corrective action taken.

- All requests, both authorized and unauthorized, for protected objects (programs, data, and transactions) should be logged.

  - The date, time of day, user identification, terminal identification, particular protected object accessed, and nature of the access should be recorded.

- Authorized actions should be reviewed regularly to ensure that the authorization is proper and that the authorized actions are appropriate.

  - It may be possible to detect if users are taking improper advantage of their authorization or if users are performing actions that are authorized but are not appropriate given the time of year or the particular job they have been assigned.

  - It may be possible to detect if the authorizations have been assigned.

  - It may also be possible to detect if the authorizations have been fraudulently manipulated or if a user's identification, authentication, and authorization have been compromised, either unbeknown to the valid and authorized user or with his knowledge.

- Unauthorized actions should be reviewed and analyzed in depth.

  - The purpose is to identify the transaction types, data, and programs that are being "attacked"; the use ID being used; the terminal being used; and the vulnerable times of day and periods during the year.

  - All individual actions and all patterns of actions should be thoroughly investigated to determine the causes of the problems, the reasons for the problems, the exact nature of the problems, and the accountable or responsible people involved.

- All modifications of sensitive data and programs should be logged.

  - The following information should be recorded: date, time of day, user identification, terminal indentification, the particular protected object that was modified, and a "before" and "after" image of the protected object.

  - This log should be reviewed in detail.

  - Each entry should be reviewed for appropriateness, authorization, and accuracy. If any inappropriate, improper, unauthorized, or inaccurate modifications are detected, they should be investigated immediately and corrective action taken.

  - Again, it is necessary to analyze the individual entries as well as the patterns of inappropriate, improper, and unauthorized modifications.

  - The "before" and "after" images will facilitate the review, make it possible to identify faulty processing, and make reconstruction or restoration of the protected object easier to perform.

- Listings of all security-procedure violations should be prepared daily.

  - The listings should contain an analysis of the violations and summary statistics (such as the number of violations and errors committed by each user, at each terminal, on each type of protected object, on particular protected objects) that would highlight unusual and suspicious activities and patterns of activities.

- Histories of security-procedure violations should be maintained. Summaries and statistics relating to the types of violations committed, when the violations were committed (most vulnerable time of day, week, or month for all

violations and for specific types of violations), who committed the violations, and similar information should be prepared.

- Such statistics and summaries will highlight patterns of unauthorized activities over a period of time.

- Patterns may emerge that might not otherwise be suspected or detected.

- Daily and historical listings and logs of all changes to user identifications, authentications, authorizations, security codes, file passwords, etc. should be prepared.

  - The listings and logs should be scrutinized by authorized management to ensure that all such changes were proper, appropriate, authorized, and performed by authorized personnel.

  - Any suspicious, unauthorized, improper, and inappropriate changes must be investigated immediately. Patterns of suspicious, unauthorized, improper, and inappropriate changes must also be investigated.

- All temporary authorizations (ones granted in special situations when access to particular protected objects is needed but the authorized user or terminal is not available) must be logged.

  - In addition, such temporary authorizations must be carefully administered and closely monitored.

- The security of the logs must be preserved. This is equally true when they are on-line, when they are being processed, when they are being printed and distributed, and when they are in the possession of the authorized security officers and of management.

- When they are on the system, they must receive higher security than the most sensitive data files, data bases, and programs.

- When they are in hard-copy form, they must receive the same attention as the most confidential reports.

- They must not be left lying around on desks or in unlocked cabinets; they should be kept under lock and key.

- They should not be thrown out with the trash. They should be shredded or burned prior to disposal.

6. AN EXAMPLE OF A SPECIFIC SOFTWARE SECURITY SYSTEM: RACF

- IBM's Resource Access Control Facility (RACF) is one example of a data/software security system that provides user identification and authentication, authorization, and surveillance controls. Exhibit IV-5 presents an overview of RACF.

- The RACF features will be briefly discussed in the following areas:

  - User identification and authentication.

  - Authorization.

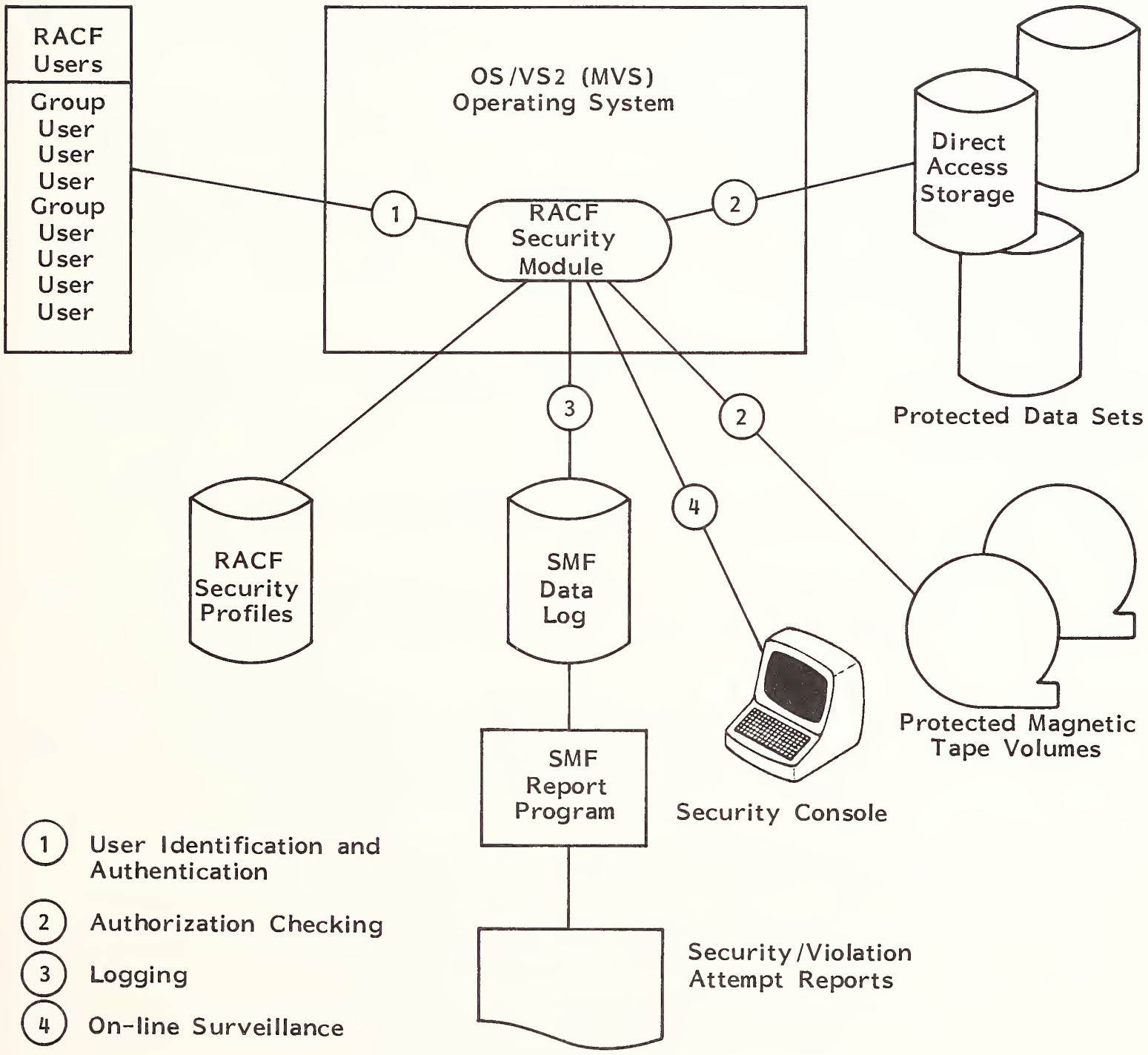
  - Surveillance.

- RACF performs user identification by user ID and authentication by password.

- RACF maintains security profiles for each user, for each group of users who have the same access authorizations, and for each protected data file.

EXHIBIT IV-5

OVERVIEW OF RACF



- The security profiles are maintained on a direct access device, labeled "RACF Data Set" in Exhibit IV-5. The profiles contain the attributes of the user, group of users, and protected data file, as well as the authorization specification (function, such as read or modify, and protected object) for each protected data file.

- Thus, the users are explicitly authorized to access particular data files and to perform specific functions on those data files.

- RACF logs all authorized and unauthorized attempts to access the system and to access particular data files. This logging is performed by recording all system and data accesses in the SMF (System Management Facilities) Data Set. (The SMF Data Set typically contains job accounting and system utilization information.)

  - RACF also records, on the security console, all unauthorized attempts to access the system, and all authorized and unauthorized attempts to access protected data files.

7. SAFEGUARDS FOR COMMUNICATIONS LINES

- Communications lines, whether they are dial-up, leased, or satellite or radio microwave links, are vulnerable to penetration and interception.

  - It is difficult, if not impossible, to physically secure the communications lines. There are, however, steps that can be taken to reduce the exposure.

- This section has been divided into two subsections:

  - Threats and penetration techniques.

  - Controls and safeguards.

- Some of the more common threats and penetration techniques will be discussed, as well as some of the available controls and safeguards to prevent the penetration and minimize the exposure resulting from penetration.

- The perpetrator's ability to successfully penetrate a communications network depends on several factors, including his technical knowledge of both telecommunications and the system he is attempting to penetrate, and his access to or possession of the necessary interception, penetration, and monitoring equipment.

- The more common penetration techniques are:

  - Masquerading.

  - Eavesdropping.

  - Piggybacking.

  - Between lines.

  - Line grabbing.

- Masquerading.

  - A perpetrator may pretend to be an authorized user and may attempt to gain access to a computer system and its data as that user.

  - The perpetrator would have had to obtain the user's identification and authentication information by some means in order to perform this technique.

- Eavesdropping.

  - This involves tapping or cutting in on a communications line, or on a satellite or radio (terrestrial) microwave link.

  - It is often referred to as "passive" infiltration. It is passive in the sense that the perpetrator only listens (or records), but does not interfere with the transmission.

- Piggybacking.

  - The perpetrator inserts a special terminal into the communications line, then intercepts the transmission between the user and the computer system.

  - The perpetrator may intercept the user's input and modify it, or completely replace it before sending it to the computer system.

  - The perpetrator typically transmits an error message to the user indicating that the system is not available or has gone "down."

  - This technique is often referred to as "active" infilitration.

- Between lines.

  - The perpetrator inserts a special terminal into the communications line. The perpetrator then accesses the system whenever the authorized user is connected to the computer but is inactive.

  - During any particular terminal session (i.e., the time period during which an authorized user is signed onto the system) there will be short periods of time during which the authorized user will not be actively sending and receiving information.

- It is during such periods of inactivity that the perpetrator goes to work, taking advantage of the communications line that has already been established.

- Line grabbing.

  - The perpetrator inserts a special terminal into the communications line.

  - He eavesdrops on the line until the authorized user signs off the terminal. The perpetrator intercepts the user's sign-off, preventing the message from reaching the system.

  - He transmits the expected system sign-off message to the user. Then he uses the one he "grabbed" from the authorized user to access the system.

- The controls and safeguards that exist in a communications environment are:

  - Physical security.

  - Encryption.

  - Authentication checks.

  - Transaction serial numbering and "time stamping."

  - Automatic terminal disconnect.

  - Call-back procedures.

- Other measures, including user identification and authentication, terminal identification, and authorization.

- Physical security.

  - It is virtually impossible to physically secure public communications lines and microwave communications.

  - However, there are some steps that can, and should, be taken. These steps should be taken in addition to physically securing your data processing installation and terminal locations.

  - There are only certain points in a communications network where wiretapping is not extremely difficult.

    . One of the best places from a perpetrator's standpoint is the telephone closet.

    . Users frequently make the job easy for the wiretapper by prominently labeling their data communications lines.

    . Users should, therefore, physically secure their telephone closet and carefully restrict access to it.

  - Communications lines that exist solely on the user's property should be buried in metal conduits in concrete-filled trenches. This will inhibit wiretapping by making the communications lines inaccessible to the wiretapper.

- Encryption.

  - Encryption is the process of transforming the data transmitted over the communications and microwave links to render it unintelligible during transmission.

- The transformation may be accomplished by transposition of the characters in the data or message (scrambling), substitution of the characters with other characters or groups of characters, or logical, arithmetic, and algebraic manipulations of the characters in the data or message.

- Encryption may provide the only secure way to protect your passwords and data during transmission, especially where microwave communications links are used. Encryption will be discussed at length in the next section.

- Authentication checks.

  - A code may be inserted into each message sent to and from the computer system that would in some way provide authentication to the user and the computer system that messages were not being intercepted, rerouted, or introduced by an illegal, intervening terminal.

  - The code may be a sequential message number or it may be generated using an algorithm driven by characters of the previous message.

- Transaction serial numbering and "time stamping."

  - With this technique, the computer assigns a unique sequential identification number (and also, in some systems, a date and time of day) to each transaction received from terminals (and also, in some systems, the before-and-after version of the data base records affected by the transactions).

  - Often the terminal operator will also have this identifier displayed on his terminal. The transactions with their appended serial numbers are recorded as they occur on a tape or disk known as a transaction log or journal.

- The process of number tagging and logging is sometimes called "journalizing."

- Journalizing serves a number of purposes.

  . One common use is in reestablishing system operations after a failure where the journal is used to determine the last transaction processed before the failure.

  . The journal is also used to aid in the analysis of system errors and suspicious events and, in this sense, is part of the audit trail for on-line systems.

  . Some on-line systems perform what is called a "memo-posting" or "shadow-posting" function which updates a copy of the master file or data base during daytime on-line operations. At night, during batch operations, the original (actual) master file or data base is updated, often using the journal as a source of transactions and the before-and-after records as a control feature (for comparison).

- Automatic terminal disconnect.

  - The computer system software, using the hardware clock or timing mechanism, should automatically disconnect a terminal from the computer system after a pre-determined period of inactivity.

  - Users should not, however, rely on this feature. They should disconnect the terminal themselves when they have finished their session.

  - This feature is important because it prevents an unauthorized user from accessing the system by using a terminal or communications line

already connected to the system that has been abandoned by the authorized user.

- Call-back procedures.

  - Call-back procedures are, in a sense, an authentication scheme in which the computer system verifies that the user is, in fact, who and where he says he is.

  - The user signs onto the system and enters his user identification and authentication. The computer system establishes the user's identification and terminal location. It then disconnects the user and "calls back" the identified terminal. The communication line established by the computer system (not the user) is the one actually used for the terminal session, the purpose being to ensure that the user is at an authorized terminal in an authorized terminal location.

  - It is a particularly useful safeguard in a communications environment that uses dial-up rather than, or in addition to, leased lines, because the user could be calling the system from any location, authorized or unauthorized.

  - Call-back procedures may be implemented in other ways as well.

    . For example, the user may sign onto the computer system and the computer system may call him back using a separate line without disconnecting him to verify that he is, in fact, accessing the system. The user would respond by actuating a switch on the terminal.

- Other measures. There are other controls that were discussed earlier in this chapter. Among these are:

- Identification and authentication, especially techniques that make masquerading difficult.

- Terminal identification, especially when used as one aspect of authorization specification.

- Authorization, especially techniques such as password-protected data and programs, where an additonal "layer" of security is provided.

    . With such techniques, knowing or having an authorized user's identification and authentication does not give you access to all the protected objects the user is authorized to access.

    . The passwords securing the protected objects must also be known.

8. ENCRYPTION SYSTEMS

- Data transmitted over communications lines and over radio and satellite microwave communications links, and data stored within the computer system are vulnerable to unauthorized and fraudulent access, use, and modification. We have discussed ways to protect data stored on your system. Encryption techniques used in conjunction with the other controls discussed can provide additional security for your data and data bases. Recognize, however, that these techniques are usually uniquely defined for each installation unless the National Bureau of Standards Data Encryption Standard (discussed elsewhere in this report) is employed.

    - In a data communications environment where there is little, if anything, you can do to secure the communications lines and microwave links, encryption may provide the only practical way to protect your data.

- Encryption is, in essence, the transformation of a message or of data for the purpose of rendering it unintelligible.
  - The transformation may be effected by transposition (changing the order of the characters in the message or the data), by substitution (replacement of the characters in the message or the data with one or more different characters), or by arithmetic, algebraic, and logical manipulation of the message or the data.
- The elements involved in encryption are the original version of the message or data, known as plaintext or cleartext; the transformed version of the message or data, known as ciphertext; the algorithm, or method by which the message or data is transformed; and the key, a pattern of characters or bits that serves as a secret parameter in the encryption and decryption processes.
- The discussion of encryption will be divided into the following topics:
  - Types of encryption.
  - Types of encryption systems.
  - Data Encryption Standard.
  - Encryption implementation.
  - Cryptanalysis.
  - Generation, administration, and distribution of keys.
- There are two basic types of encryption:
  - Reversible encryption.
  - Irreversible encryption.

- Reversible encryption.

  - In a data communications environment the sending location, which may be a terminal or a computer, encrypts or encodes the data and transmits it to the receiving location.

    . The receiving location decrypts or decodes the ciphertext, thereby returning it to its original form.

    . Reversible encryption, therefore, involves the encryption of plaintext into ciphertext and the decryption of ciphertext into plaintext.

- Irreversible encryption.

  - Irreversible encryption involves only the encryption in plaintext into ciphertext. The ciphertext cannot be decrypted.

    . Irreversible encryption is useful for protecting security profile data such as passwords and PINs used to authenticate a user's identity in data communications and consumer-oriented EFT environments.

    . Even if a perpetrator were able to penetrate the computer security system and gain access to the user identification and authentication files, he still would be unable to masquerade or gain access to the system as an authorized user.

    . The terminals used in this type of encryption environment require that the data be entered in its original (plaintext) form.

- There are several different types of encryption systems. For illustrative purposes, we will identify a few of them and will discuss their strengths and weaknesses. The encryption systems that will be discussed are:

- Transposition.
- Monoalphabetic substitutions.
- Polyalphabetic substitutions.
- Codebook substitutions.
- Vernam system.

- Tranposition.
  - Tranposition involves the rearrangement of the characters in the data or message according to some predetermined rule.
  - The same characters appear in both the plaintext and the ciphertext, however, they appear in different positions.
  - The number of characters in the plaintext and the ciphertext is the same. This type of transformation is often called "scrambling."
  - Because there is such a great relationship between the plaintext and ciphertext, transposition is not an effective way of securing data.

- Monoalphabetic substitutions.
  - Monoalphabetic substitutions involve the replacement of each character in the data or message by a corresponding character in the cipher alphabet. Monoalphabetic substitutions use only one cipher alphabet for encryption and decryption.

- Thus, there is a one-to-one correspondence between the letters in the plaintext alphabet and the letters in the cipher alphabet.

- An example of monoalphabetic substitution is presented in Exhibit IV-6.

- Encryption is performed by finding each character of the plaintext in the plaintext alphabet and finding the corresponding character in the cipher alphabet. Thus, PASSWORD becomes KZHHDLIW.

- Decryption is performed by locating the characters of the ciphertext in the cipher alphabet and finding the corresponding characters in the plaintext alphabet.

- Monoalphabetic substitution is not a secure encryption system. Because there is a one-to-one correspondence between the plaintext alphabet and the cipher alphabet and because English, as well as most other languages, is highly redundant, it is easy for an amateur cryptanalyst (codebreaker) to decrypt the ciphertext.

- The method used to break the code involves performing frequency analyses on the individual characters, pairs (begrams), and trios (trigrams) of characters in the ciphertext.

- The results of the frequency analyses are compared to frequency analyses of the occurrence of individual characters and pairs of characters in the English language. Such frequency analyses are readily available.

- An expert cryptanalyst can break a monoalphabetic system with a single message containing 40 to 60 characters.

EXHIBIT IV-6

MONOALPHABETIC SUBSTITUTION

Plaintext Alphabet: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher Alphabet:: Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Sample Encryption:

Plaintext: P A S S W O R D

Ciphertext: K Z H H D L I W

Sample Decryption:

Ciphertext: H V X F I V W

Plaintext: S E C U R E D

- Polyalphabetic substitutions.

  - Polyalphabetic substitutions differ from monoalphabetic substitutions in that they use two or more cipher alphabets in a predetermined pattern to perform the encryption and decryption.

  - Thus, if two cipher alphabets are used, the odd characters (i.e., first, third, fifth, . . .) of the plaintext might be encrypted using the first cipher alphabet, and the even characters (i.e., second, fourth, sixth, . . .) might be encrypted using the second cipher alphabet.

  - Exhibit IV-7 illustrates a polyalphabetic substitution using four cipher alphabets.

  - In the exhibit, the "P" is encrypted using the first cipher alphabet, the "A" using the second, the "S" using the third, the "S" using the fourth, the "W" using the first, the "O" using the second, and so on. Thus PASSWORD becomes QCVWXQUH.

  - The standard method of breaking a polyalphabetic substitution code involves deducing the number of cipher alphabets used and then performing the frequency analyses described for monoalphabetic substitution on the characters believed to be encrypted using the same cipher alphabet (the first and fifth characters, second and sixth characters, etc., in our example).

  - An experienced cryptanalyst would need 40 to 60 characters of ciphertext for each cipher alphabet. Thus, he would need 160 to 240 characters of ciphertext to break this code.

  - Polyalphabetic substitution, although more secure than monoalphabetic substitution, is nonetheless not a very secure encryption system.

EXHIBIT IV-7

POLYALPHABETIC SUBSTITUTION

Plaintext Alphabet:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cipher Alphabet 1:	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
Cipher Alphabet 2:	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
Cipher Alphabet 3:	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Cipher Alphabet 4:	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

Sample Encryption:

Plaintext:	P A S S W O R D
Ciphertext:	Q C V W X Q U H

- Codebook substitutions.

  - Codebook substitutions involve the use of a codebook or dictionary which relates the plaintext elements (characters, words, phrases) to the ciphertext elements, referred to as code groups.

  - Codebook substitutions generally operate on elements of the plaintext that are variable in length, such as syllables, words, phrases, or sentences. Each element of the plaintext is looked up in the codebook or dictionary to determine its code group, the corresponding ciphertext element.

  - An example of a portion of a codebook is shown in Exhibit IV-8.

  - There are several disadvantages to codebook substitutions.

    . One disadvantage is that, as with monoalphabetic and polyalphabetic substitutions, codebook substitutions are vulnerable to analysis by experienced cryptanalysts.

    . Another is that the codebook may be compromised which means that the encryption system has been compromised. This is particularly true if the codebooks are in printed form. Thus, new codebooks might have to be issued very frequently.

    . If the codebook is stored on the computer system, it is still vulnerable to compromise.

    . In addition, either the plaintext-ciphertext combinations would have to be very limited or the codebook would require a tremendous amount of storage space and the codebook look-up would be time consuming.

EXHIBIT IV-8

CODE BOOK ENCRYPTION TABLE

CODE GROUP	PLAINTEXT
3964	Emplacing
1563	Employ
7260	En-
8808	Enable
3043	Enabled
0012	Enabled to

- Vernam system.

  - The Vernam system is a key-additive system.

  - The key is a string of Os and Is. The key is added using modulo-2 (exclusive-or) addition to the bit pattern of the plaintext, thereby producing the cipertext.

  - To decrypt the ciphertext, the same key is added, modulo-2, to the cipertext. This is illustrated in Exhibit IV-9.

  - The key may be a sequence of random numbers, pseudo-random numbers, or characters.

  - It may be a block cipher, meaning that a single block or quantity of plaintext is enciphered into a single block of output.

  - Exhibit IV-9 used a block cipher of 12 bits. If the plaintext were 24 bits long, our block cipher, modulo-2, would have been added to the first 12 bits of the plaintext, then to the second 12 bits of the plaintext.

  - The key may also be a stream cipher, meaning that the string of bits (bit stream) is very long and the entire string is added, one bit at a time, modulo-2, to the plaintext without requiring repetition of the key. Key generation will be discussed later in this section.

- The degree of security provided by key-additive encryption is dependent upon the randomness and the security of the key.

- The National Bureau of Standards adopted a standard encryption algorithm in November 1976.

EXHIBIT IV-9

KEY ADDITIVE ENCRYPTION

Encrypt:

Plaintext:	100	110	101	110
Key*	010	101	010	101
Ciphertext	110	011	111	011

Decrypt:

Ciphertext	110	011	111	011
Key*	010	101	010	101
Plaintext:	100	110	101	110

* Key is based on a module 0-2 addition (exclusive - or) and followed by:

1 + 0 = 1
0 + 1 = 1
1 + 1 = 0
0 + 0 = 0

- The encryption algorithm was developed and patented by IBM and is called the Data Encryption Standard (DES).

- DES is a reversible encryption system; the sending location encrypts the data or message and the receiving location decrypts the ciphertext.

- How it works.

  - DES uses a recirculation block product cipher.

  - The key consists of 64 bits, 56 bits for the key and 8 bits for parity checking.

  - The DES algorithm enciphers a block of 64 bits at one time, thus the key is designed as a block cipher.

  - DES is not a simple key-additive encryption system, such as the Vernam system. Rather it uses a complex algorithm involving the following steps:

    . The plaintext block of 64 bits is subjected to an "initial permutation," which, in essence, is a transposition of the bits according to a predetermined rule.

    . The permuted plaintext is then subjected to a rather involved key-dependent computation involving several more permutations of the input as well as of the key, modulo-2 arithmetic, and table look-ups. This process is repeated 16 times. It produces what is referred to as the preoutput, a 64-bit block.

    . The preoutput is subjected to a final permutation, transposition, which is the inverse of the initial permutation.

- Degree of security.

  - DES is highly secure but not unbreakable.

  - The security of DES is totally dependent upon the security of the 64-bit key. The algorithm has been published in numerous publications.

  - Just how secure DES actually is has been the subject of some controversy. The controversy revolves around whether or not the size of the key is adequate for security purposes.

- Whitfield Diffie and Martin Hellman of Stanford University contend that the length of the key should be increased, perhaps doubled. They maintain that a machine capable of "breaking" the key could be built for approximately $20 million.

  - The method used to break the key would be brute force, that is, trying every possible combination of 56-bits (with 8 parity bits).

  - Whereas $20 million payout may not be cost effective for most criminally-motivated individuals, it may be cost effective to some large organizations, such as the major intelligence agencies. "(The) major intellience agencies possess the financial resources and the interest to build such a machine," say Diffie and Hellmen.

- Diffie and Hellman's concerns go a step further: "More seriously, in about 10 years' time, the rapidly decreasing cost of computation will bring the machine's cost down to the $200,000 range and the cost per solution down to the $50 range. The standard will then be almost totally insecure."

  - The current cost per solution (i.e., cost to find one key, assuming that the key is changed daily) is estimated to be $5,000.

- Others who agree with Diffie and Hellman's suggestion that the key is too short to provide adequate security feel that the plaintext should be double-encrypted (i.e., encrypted twice with two different 64-bit keys).

  - This double encryption would essentially provide the same level of security as doubling the size of the key.

  - Doubling the size of the key would result in a cost per solution of $\$2 \times 10^{25}$.

- Those who feel that DES provides the necessary level of security counter their opponents' arguments on the followng grounds: (1) $20 million would be very difficult to obtain; therefore, the method for breaking the key is cost prohibitive; (2) the accumulation of the necessary LSI chips to build the machine would arouse suspicion; and (3) there would be difficulties with component reliability, cooling, and obtaining sufficient electrical power to run the machine, which would doom the effort.

- The National Bureau of Standards (NBS), while committed to DES, nevertheless realizes that technological advances may impair the security provided by DES. They expressed the following qualification: "The protection provided by this algorithm against potential new threats will be reviewed within five years to assess its adequacy. In addition, both the standard and possible threats reducing the security provided through the use of this standard will undergo continual review by NBS and other cognizant federal organizations. The new technology available at that time will be evaluated to determine its impact on the standard. In addition, the awareness of any breakthrough in technology or any mathematical weakness of the algorithm will cause NBS to reevaluate this standard and provide necessary revisions."

- The controversy about DES has been useful in the sense that it has made people aware of several important considerations about encryption systems in general--key length and the importance of randomly generating the keys and protecting access to them.

- There are national security systems that involve intelligence data for which DES would not be suitable.

  - However, for the vast majority of commercial and governmental systems, DES should provide an appropriate level of protection and avoid the problems that would arise from the incompatibility of competing systems.

  - Few technical developments in the EDP world are viewed as having extraordinarily long lives and we would remind our readers to expect a need to change some years in the future, as indicated in the NBS statement above.

  - The master system breaker who is able to execute successfully a large-scale fraud will gain his knowledge by exploiting a variety of security and control weaknesses that are far more vulnerable than DES.

- There is no question that the proper administration of the key, discussed later in this section, will go a long way to making DES "unbreakable" in practice, if not in theory.

  - The cryptographic algorithm transforms a 64-bit binary value into a unique 64-bit binary value based on a 56-bit variable.

  - If the complete 64-bit input is used(i.e., none of the input bits should be predetermined from block to block) and if the 56-bit variable is randomly chosen, no technique other than trying all possible keys using known input and output for the DES will guarantee finding the chosen key.

  - As there are over 70,000,000,000,000,000 (seventy quadrillion) possible keys of 56 bits, the feasibility of deriving a particular key in this way is extremely unlikely in typical threat environments.

- Moreover, if the key is changed frequently, the risk of this event is greatly diminished.

- However, users should be aware that it is theoretically possible to discover the key in fewer trials (with a correspondingly lower probability of success depending on the number of keys tried) and should be cautioned to change the key as often as practical.

- Users must change the key and provide it a high level of protection in order to minimize the potential risks of its unauthorized computation or acquisition.

- Encryption systems may be implemented in software and hardware.

  - Various systems are available commercially, including vendor-proprietary systems and DES.

  - The commercially available software encryption systems vary in terms of processing overhead and system degradation.

- Hardware encryption systems are also commercially available.

  - DES may be implemented in hardware, as well as in software.

  - The encryption system is typically contained on an electronic "chip."

- Hardware encryption systems are incorporated into a number of special-purpose terminals.

  - Microprocessors containing the encryption system may be appended to certain terminals.

- Encryption devices may also be inserted at modem interfaces. Two specific areas where this can happen include:

  . Link encryption.

  . End-to-end encryption.

- Link encryption.

  - The encryption devices are placed at the modem interfaces. Encyption and decryption is performed in a manner that is transparent to the receiving and sending stations.

  - Link encryption is adequate for protecting against wiretapping, but in a network, it does not guard against misrouting.

  - In a network which contains a routing (switching) function, this switch handles cleartext and if a message sent from A to B is misrouted by the switch to C, the message is intelligible to the user at C because it has been decrypted, using the key that deciphers the encryption at that station.

  - Thus, link encryption will not provide protection against intentional or unintentional misrouting in a switching network.

- End-to-end encryption.

  - Performed with either hardware or software, end-to-end encryption involves encryption performed by the sending station and decryption performed by the receiving location.

  - the encrypted message can only be decrypted by a receiving location that has the appropriate key. Thus, the message is protected if it is inadvertantly or deliberately misrouted.

9. CRYPTANALYSIS

- Cryptanalysis is the process of analyzing encrypted messages for the purpose of recovery the original (plaintext) message without using the means available to the legitimate recipient.

  - Cryptanalysis is thus the penetration of the encryption system.

  - The perpetrator is known as the cryptanalyst.

- Without proper administration and a good encryption system, encryption may provide a false sense of security.

  - The greatest threat to encryption systems is human ingenuity and diligence, particularly the human ingenuity and diligence of the experienced cryptanalyst.

  - History has shown that if an encryption system can be broken, it will eventually be broken.

  - This is not meant to imply that encryption is any less important as a security measure. The emphasis is on "eventually."

  - Not all encryption techniques provide the same degree of security; proper administration of your encryption system is of the utmost importance in preserving the security it provides.

  - You cannot simply implement an encryption system and then ignore it because you assume that you are protected.

- The most important elements of cryptanalysis (for the purposes of this discussion) are the length of the intercepted message, available computational resources, time, and the work factor.

- The longer the ciphertext message that the cryptanalyst has to work with, the greater the probability the he will be able to break the system.

- If the intercepted ciphertext is too short, even an expert cryptanalyst with sophisticated resources and an abundance of time may never be able to break the code.

- Work factor relates to the amount of effort, time, and resources required to break the code.

- If the work factor is very high, meaning that a tremendous amount of human and computational resources are needed to break the system, the system is considered to be strong.

- How can the user assess the strength of a current or prospective encryption system? There are several ways:

  - Experts in the field of cryptanalysis should be consulted whenever you decide to design your own encryption system.

  - Experts in the field of cryptanalysis should be asked to validate your current, new, or prospective encryption system. After extensive analysis they will be able to tell you whether your system is very difficult to break.

    . Thus, they will tell you what the relative work factor is.

    . They will not be able to determine if penetration of your system is absolutely impossible.

- In most encryption systems the algorithm remains fairly constant.

  . The key is the crucial variable.

  . If you have a strong. secure encryption system, the cryptanalyst should be able to know the algorithm and have a plaintext message and its corresponding ciphertext and still not be able to break the code.

  . The work factor then relates to the effort and resources expended to derive the key.

  . You can significantly increase the work factor by decreasing the amount of time that is available to the cryptanalyst by changing the key on a regular basis.

  . Since the key is the crucial element, if it is generated properly and distributed and maintained in a very secure manner, then every time it is changed, the cryptanalyst must start the analysis from ground zero.

- As mentioned earlier, the strength of, and the security provided by, an encryption system is often dependent upon the security of the key.

  - The report will now examine:

    . Key generation considerations.

    . Key administration considerations.

    . Key distribution considerations.

- Key generation considerations.

  - It is generally acknowledged that whenever the key size (the number of bits that make up the key) is equal to, or greater than, the input size (the number of bits that make up the plaintext input), it is possible to construct an encryption system that is "unbreakable" in practice, if not in theory.

  - Each bit of the key is used once, and only once, to encipher each bit of the input.

  - This type of key is referred to as a stream cipher, a once-only key, or a one-time tape key.

  - A once-only key may be produced on paper tape, magnetic tape, or a disk.

    . The medium on which the key is produced is dependent upon the equipment at the receiving and sending locations in the communications environment.

    . All the receiving and sending locations must have a copy of the appropriate key and the encryption algorithm in order to encrypt the plaintext to be transmitted and to decrypt the ciphertext that is received.

  - Such once-only keys or stream ciphers are not pratical in all situations. Thus, a block cipher or periodic key may be used.

    . This key enciphers a block of input equal to the size of the key.

    . The same key is used over and over to encipher a plaintext message.

- Regardless of whether an "infinite" stream cipher (once-only key) or a "finite" block cipher is used, the single most important consideration in generating the key is that it be as nearly random as possible.

  . There must be no predictable relationship among the bits of the key.

- Pseudo-random number generators are often used to geneate the key. Not all pseudo-random number generators are equally effective in generating numbers that appear to be truly random. Therefore, extreme care should be taken when choosing a pseudo-random number generator.

- The initial seed used to start the pseudo-random number generator may be derived (through selection of certain characters, computation, etc.) from the user's authentication password, from the user's identification, from message length, or from any number of constant or variable values.

  . The initial seed has to either be communicated to or be determined in some way by the receiving location.

- The pseudo-random number generator is a method of key generation using software.

  . Keys may also be generated by hardware, using linear shift registers and a series of exclusive-or and transposition operations, or by special cryptographic hardware.

  . Again, the overriding consideration is that the bit pattern of the key be as nearly random as possible.

- Key administration considerations.

  - The need to change the keys periodically has been discussed throughout this section. Changing of the keys in a controlled and regular manner can effectively make your encryption system unbreakable.

    . For example, if it would take an experienced cryptanalyst one year or more to determine your key, and you change the keys quarterly, the cryptanalyst could make no practical use of the keys.

    . Thus, the recommended frequency of changing keys is partially based on the estimated work factor associated with breaking the key.

  - Another consideration is the potential loss resulting from a compromised key.

    . In some national and international EFTS environments, where large-dollar-value money movements are involved, the potential loss may be extremely great.

    . In such environments, it may be desirable to change the key as often as once or twice each day.

    . The potential loss need not be a direct loss. It may also be the loss or compromise of data.

    . Thus, the data requirements may necessitate a very frequent changing of the key.

    . The key must also be changed whenever it is suspected to have been compromised.

- Key distribution considerations.

  - Utmost care must be taken when distributing keys to ensure that the key is not compromised or exposed during distribution.

  - Depending on the equipment used, the key may be produced on paper tape, magnetic tape, disk, plug-in module, magnetically encoded card, or almost any other available medium.

  - They may be sent by registered mail or transported by company courier.

  - Depending on the equipment used, they may also be transmitted through the communications network.

  - Whenever the key is distributed, regardless of the method of distribution, utmost security precautions must be taken.

    . It may be desirable to transmit multiple keys and to indicate which key is to be used at another time.

    . Alternatively, it may be desirable to send bit streams to two different people at different times. Each bit stream is loaded into the encryption device and the modulo-2 addition of the bit streams produces the actual key.

  - If the equipment in the communications environment has been equipped with key generation hardware or software, it is frequently necessary to distribute the seed for the generation algorithm.

    . Again, distribution may be by registered mail, by company courier, or by transmission through the communications network.

. The utmost security precautions are necessary.

. It may be desirable to distribute multiple seeds at one time and, at another time, distribute an indication of which seed is to be used.

- In systems that are terminal-security rather than user-security oriented, the down-line loading of the new key may be accomplished by transmitting the new key encrypted by the current key.

. Once a perpetrator discovers one key, he can readily obtain the others.

. A way to reduce the odds of such a compromise is to transmit new keys encrypted by a key that is only used for this purpose.

. Since this special-purpose key is used much less often than the one employed for routine transmission, the cryptanalyst would be faced with a much higher work factor in trying to break the system.

- If in any of the methods of key or seed distribution discussed thus far the transmittal appears to have been tampered with, the computer security officer should be notified immediately.

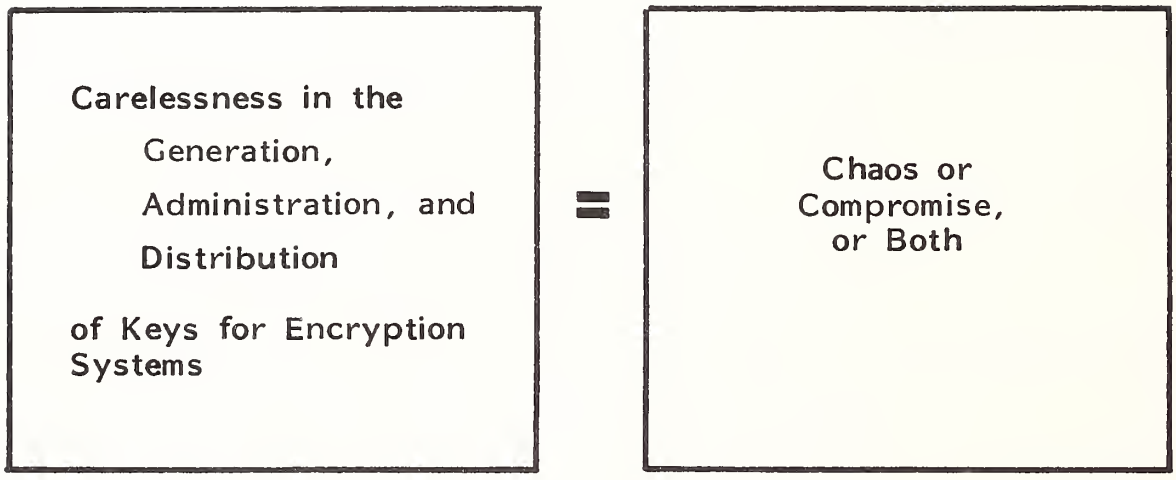
. Depending on the circumstances, it may be necessary to regenerate and redistribute the keys or seeds.

10. CRYPTO SYSTEMS SUMMARY

- In this chapter, we have introduced a number of concepts that are of fundamental importance in the generation, administration, and distribution of keys for encryption systems. These are summarized in Exhibit IV-10.

EXHIBIT IV-10

CRYPTO SYSTEM SUMMARY



- It should be evident that detailed procedures and controls must be fashioned to suit the particular characteristics of a given application.

- It should also be evident that where security is concerned, casual attitudes and carelessness cannot be tolerated under any circumstances.

V DATA SECURITY

V DATA SECURITY

A. TECHNOLOGY OVERVIEW

- Security functions have to be carried out in two timeframes. The first is immediate; the second is retrospective.

  - The immediate detection is accomplished by threat monitoring; in this connection, the use of a security console can be of assistance.

  - Retrospective detection requires the analysis of user trends to identify deviant behavior and the establishment of audit trails.

- A computer should possess the capability to log, in machine sensible format, the details of all apparent violations of security and to scan these logs and retrieve information selectively from them.

- The transactions upon which attention should focus include: entry into the system, entry to sensitive files, execution of certain specified programs, and allocation of systems resources, such as peripheral storage devices containing sensitive information as well as all input and output transactions.

- The recording of these security transactions should be accomplished in such a way that the log is protected against unauthorized intervention by the operator, users, or systems personnel.

- A good case can be made for the use of a dedicated minicomputer to control the logging function. Management can control minicomputers easier than they can control terminals.

- How to recognize a security violation is an immediate problem. Certain events deserve to be viewed with suspicion in this regard.

  - These include:

    . The abnormal termination of a job.

    . An abnormal shutdown of the system.

    . Failure of any hardware or software protection mechanism.

    . Unsuccessful attempts to log on the system.

    . Unauthorized attempts to access sensitive files.

    . Unauthorized attempts to use privileged instructions or sequences of them.

    . Attempts to exceed the user's allocated address space.

    . Unauthorized attempts to access systems resources.

- When any suspicious action is observed, the recording mechanism should be able to specify the identity of the devices involved (terminal and storage device, for example), the type of violation, the identifier appropriated by the user, the date and time of the incident, and the identification of the file, program, or resource being sought.

- There is the proposition that a security officer would sit at a control console to grant or deny access to the system or any of its critical resources, but this appears to be the very antithesis of modern information systems design.

- There is merit, however, in having a console that would filter the information and give an immediate warning of incidents such as a third and unsuccessful attempt to log-on, improper response to a request for re-authentication, or an attempt to use an unauthorized instruction or instruction sequence.

- Warning could also be given of acts such as attempts to exceed authorized work space, attempts to gain unauthorized access to system resources, attempts to read newly allocated memory without first having written on it, or unauthorized attempts to enter a more highly privileged operating state.

- The security console could likewise warn of the failure of any systems-protective mechanism or of the inability of the system to verify successfully any systems program, security table, or address relocation table.

- It is a good idea to keep lists of names or other sensitive data files with dummy entries so that if the list is, for example, unlawfully sold to a direct-mail house, security personnel will become aware of the offense when solicitations are made at drop addresses intended for the invented fictitious persons.

  - With a little ingenuity all kinds of trap accounts, files, and programs can be devised to lure a perpetrator into penetrating them and thus revealing his presence.

I. ANALYSIS OF USAGE TRENDS

- There is an intellectual attraction in detecting intruders by statistics. It does, however, entail a good deal of planning and foresight. One must first develop the ability to sense significant deviations from expected patterns in systems activity and usage of resources.

- One will, at first, have to develop base data from the study of console logs, terminal logs, systems accounting records, records of hardware/software failures and subsequent restorations, and any data available from hardware or software monitor probes.

  - Naturally, systems utility programs and editing routines will have to be developed to extract the security-relevant facts from so great a mass of data.

- The products of these analyses will then be activity profiles specific to the system as a whole, to each user of the system, to each terminal, and to all sensitive files and programs.

- Exhibit V-1 suggests some of the items that might constitute an activity profile and relates them to the specific profiles in which they would be most applicable.

  - There is an implicit time dependency connected with every profile constituent.

2. MORE ON AUDIT TRAILS

- An EDP system should be capable of constructing an audit trail of all accesses to sensitive information and use of critical resources.

  - Documentary evidence must be retained so that each step of an audit trail can be independently confirmed.

- In a system that deals with highly sensitive material, one should be able to develop the employment history of any given staff member in respect to access privileges internal to the computer system having been granted, altered, or revoked.

EXHIBIT V-1

SECURITY ACTIVITY TRACKING TABLE

INCIDENT	SYSTEMS	USERS	TERMINALS	FILES	PROGRAMS
Restarts	X				
Unsuccessful Log-Ons	X				
Communications Errors	X				
Program Reruns	X				
Hardware/Software Failure	X				
Down Time (Per Shift)	X				
Successful Log-Ons		X	X		
CPU Time		X	X		
Security Incidents		X	X		
Changes in Authorization Table		X	X		
On-Line Memory Residence		X			
File Accesses		X			
Instructions (Per Job)		X			
Supervisor Calls (Per Job)		X			
I/O Requests (Per Job)		X			
Connect Time (Per Job)			X		
Read (Per Job)				X	
Write (Per Job)				X	
Unsuccessful Executions					X
Successful Executions					X
Time Per Execution					X
Output Per Run					X

- Similarly, one should be able to develop the history, location, and current status of any access-control item used internally within the system (e.g., passwords and password lists).

- An audit trail should include the following features, irrespective of the security level of a system.

  - It should be possible, regarding any sensitive file, to go back at least six months and reproduce the transactional history of any given record.

  - It should be possible to reconcile transactions with authorizing documents for a minimum of three machine-sensible generations of any data file.

  - It should be possible to reconstruct the history of any sensitive system or application program with respect to its development and testing, implementation, maintenance, utilization, and modification.

- The best answer to the detection of computer infiltration is in the maintenance of detailed records regarding activity at an EDP center, and by reduction of data by heuristically based programs which are valid within the local context, thus obtaining evidence of penetration or defalcation.

- Exhibits V-2 and V-3 enumerate 20 danger signals that may serve as an initial checklist for anyone vested with the responsiblity of detection of computer crime.

3. SECURITY VIOLATION DETECTION

- Since software mechanisms are more easily deceived than hardware mechanisms, it is imperative that as many system security features as possible should be implemented in hardware.

EXHIBIT V-2

DANGER SIGNALS (Part I)

- Compromise of Classified Information
- Loss of Any Sensitive Asset
- Unexplained Operator Intervention in the Running of Any Job
- Presence of an Intruder
- Unexplained Absence of Any Person Possessing Access to Sensitive Information
- Unexplained Appearance of Trap Names on an Extra-Department File
- Attempts to Access Trapped Records or Files or Use of Trap Passwords
- Unexplained Increases in Systems Usage, Especially During Off Hours or Normally Silent Periods

EXHIBIT V-3

DANGER SIGNALS (Part II)

- Loss of Identification, Access Control, or Recognition Items, or Unauthorized Use of Same
- Unexplained Client Complaints Regarding Events, Including Improper Billing, Misaddressing, Incorrect Balances, or Omitted, Improper, or Incorrect Payments
- Inability to Balance Any Account
- Unexplained Inventory Shortages
- Inability to Reconcile Checks
- Unexpected Frequency of Unsuccessful Attempts to Obtain Service or Other Systems Protocol Violations
- Excessive Demands for Input or Output
- Unexplained Changes in Patterns of Communications Traffic
- Unexplained Appearance of New Code in Operating System or Utility Programs
- Unexplained Changes in Job Profiles
- Unexplained Accesses to Classified Files
- Unexpected Incidence of Hardware or Software Failures

- These should include:

  - Indication of the system's current operating state (e.g., Program Status Word) and the means for testing it.

  - Limits of the current user's address space (e.g., base, bounds, and relocation registers; partition protection lock and keys; and page and segment tables and registers) and means for testing them.

  - Means for testing the level of privilege of operation codes (e.g., command decoder).

  - Access privileges of the memory block currently in use and means for testing it (e.g., Program Control Block).

  - Contents of the current linkage segment and means for testing it (e.g., Segment Linkage Stack Register).

  - Implementation of security-relevant systems interrupts.

  - Algorithms for encrypting and decrypting text.

  - Algorithms for computing and comparing check digits.

  - Algorithms for verifying the contents of security tables and similarly sensitive memory blocks.

  - Identification of the user currently in control of the central processor and means for sensing this condition.

  - Protective mechanisms for bulk storage and the means by which this protection is implemented (e.g., permit-to-write rings and write-lock-out switches).

- Timekeeping mechanisms and means for sensing their contents and making decisions based upon such contents.

4. ON-LINE PROGRAM DEVELOPMENT

- In the process of developing and maintaining programs, there are many controls which must be imposed which are not addressed in this report.

- In an on-line environment, additional considerations need to be kept in mind.

  - On-line program development efforts must be prevented from compromising the data stored in the system and the production program libraries. Therefore, on-line programmers' activities must be controlled by the authorization system that controls the actions of all users to the system.

    . On-line programmers should be restricted from accessing live data files, data bases, and production libraries.

    . If, as a general rule, they are authorized to access particular protected objects, such authorization should be removed before on-line program development begins.

  - Specific terminals should be designated as program development terminals.

    . Such terminals should not be authorized to access the data files, data bases, and production libraries. These specific terminals, and only these terminals, should be used for on-line program development and testing.

- The security system should be able to distinguish between the execution of a program under development and of a production program.

  . The program under development should be restricted from accessing live data files, data bases, and production libraries.

- Program testing must not be performed using live data. This control is equally important if the program testing is performed on-line. If "live" data or data bases must be used to test the program, a temporary subset of the data should be created.

  . Care must be taken to prevent sensitive data from being incorporated into such temporary subsets.

  . The temporary subset of the data file of data base must be obliterated when program testing has been completed.

- The essence of these controls is to prevent the unauthorized access to the data files, data bases, and production program libraries.

  - The protected objects must be carefully secured against unauthorized modification, destruction, and disclosure. Thus, the actions of the on-line programmer should be restricted at every possible point in terms of user authorization, terminal authorization, and development program authorization.

  - The actions of the on-line programmer must also be subjected to the same surveillance as are the actions of the users of the system.

5. DATA BASE INTEGRITY

- The data base management system software and the data in the data base must be protected against unauthorized and fraudulent access, modification,

and disclosure. There are essentially two different "types" of controls that relate to data base integrity.

- Controls to maintain the integrity.
- Auditing.

- Thus far, the following types of controls have been discussed:
  - Authorization.
  - Processing controls.
  - Adjustment and error correction controls.
  - Output controls.
  - System development and maintenance controls.
  - Production system and program controls.
  - Library controls.
  - System integrity.
  - Operations controls.
  - Surveillance.
  - Others.

- In the discussion which follows, those aspects of the controls in each category that are particularly appropriate to data base integrity will be discussed.

Aspects that may have changed as a result of the use of data bases will also be identified. All the controls that remained intact will not, however, be restated.

a. Controls That Maintain Integrity

- Authorization.

  - Authorization is the mechanism by which users are permitted or denied access to particular data bases or particular data elements within the data base.

  - Authorization, in additon to specifying access permission, also specifies the functions (i.e., read, write, modify, etc.) that can be performed on the particular data elements.

  - Thus, authorization is the mechanism by which access to, modification of, disclosure of, and destruction of a data base is controlled.

- Processing controls.

  - Data editing controls, such as validity checks, reasonableness tests, range tests, and limit tests, should be performed on the data in the data base whenever the data base is updated to ensure that the data is reasonable.

  - In addition, audit trails should be produced.

    . The audit trails should contain a listing of all transactions submitted for processing.

    . The user's identification, terminal identification, date, time, an indication of whether or not the transaction was authorized, and

whether or not the transaction was processed should all be identified on the audit trail.

. A journal should also be produced. It should identify the user, the terminal, the date and time, the transaction, and a "before" and "after" image of the particular component of the data base that was updated.

- On a regular basis, validity checks, reasonableness tests, range tests, and limit tests should be performed on the data elements within the data base.

. Listings of "exception" conditions, of data elements that do not pass the tests, should be produced.

. On a regular basis the contents of the data base should be printed so that the appropriate portions can be reviewed by responsible management.

. Utmost care must be taken to ensure that the data elements are not compromised as their integrity is reviewed.

- Adjustment and error correction controls.

- It is very important that adjustments and error corrections be handled in a timely and very controlled manner.

- Output controls.

- Care should be taken by the users to protect the confidentiality of the data with which they are working.

- Terminal printouts should not be left lying around, nor should they be thrown out in the trash.

- Users should also be careful that their terminal session is not observed by an unauthorized individual.

- System development and maintenance controls.

  - The system development and maintenance controls referred to earlier apply.

  - In addition, the on-line program development controls discussed earlier in this report are necessary.

  - The programmer, when developing a new program or modifying an existing program, should only be given the relevant information for those particular data elements in the data base which his program must process. There is no need for him to know the structure of the entire data base.

  - System development must include the additional step of requesting the authorizations necessary for a particular program or system that has been tested, accepted, and approved to access other production programs and data in the data files and data bases.

    . The procedures for requesting such authorization should be formalized and should require the use of preprinted, sequentially numbered authorization request forms.

  - The data base administrator must be involved in all system development and maintenance projects involving the data bases to ensure that new production programs or modifications to existing production programs do not affect other production programs' abilities to process the necessary data in the data base.

- Production system and program controls.

  - The data base administrator should be responsible for all changes to the data base software library.

  - He should, on a regular basis, review the library to ensure that no unauthorized changes were made.

- Library controls.

  - Library controls apply regardless of whether the data resides in a data file or data base, on a magnetic tape, or on a disk.

  - When not in active use, the disks containing the data bases should be stored in the library (such as overnight and on weekends).

  - If the disks are to be sent out to be refurbished, the data bases should be obliterated prior to doing so.

- Operations controls.

  - The operators' actions must be monitored.

  - In addition, in large data base and communications systems there may be a network control center where engineers are performing equipment and line tests and monitoring the network and where programmers may be changing the polling lists and patching the communications software monitors. Their actions, too, must be monitored.

- Surveillance. The real-time surveillance and the logging discussed earlier in this report are directed toward ensuring data base integrity.

- Others. There are several other controls that relate specifically to data base integrity.

  - If authorization control is performed by the data base management system (DBMS), controls must be established to prevent all accesses to the data bases whenever the DBMS or other security software is not operational.

    . It may be necessary to physically remove the disk from the drive or to in some way preclude use of the drive.

    . Without a functioning DBMS or security software, the data base is vulnerable to uncontrolled, unauthorized, and fraudulent modification, disclosure, and destruction.

  - System utility programs should not be authorized to permit access of the data bases.

    . Whenever such programs must access the data bases (i.e., for backup purposes), a temporary authorization should be granted.

    . The processing of data bases by utility programs must be very carefully controlled.

  - The console logs should be reviewed by the data base administrator to ensure that the data bases were not accessed when the DBMS was not operational, and that the utility programs that accessed the data bases were given proper temporary authorization.

b. Auditing

- Auditing, in addition to the controls and safeguards identified above, plays a key role in ensuring data base integrity. Some of the applicable techniques include:

- Sampling.

- Integrated test facility.

- System control audit review files.

- Tracing.

- Others.

- Sampling.

  - Sampling involves the random selection of data elements for inspection purposes.

  - The intent of the sampling techniques is to uncover errors in the data base and to estimate the extent of erroneous data.

- Integrated test facility.

  - The integrated test facility (ITF) allows the auditor to add "dummy" records to the data base and to process test transactions against the "dummy" records. The test transactions are included with the live data during a normal processing run.

  - Thus, ITF enables the auditor to monitor the processing performed by production programs and to verify that processing is being performed properly.

- System Control Audit Review Files.

  - System Control Audit Review Files (SCARF) allow the auditor to monitor the processing of data by allowing him to incorporate auditor-designed tests within the production program.

  - The auditor's tests and SCARF data collection are performed on the processed data during the normal production run and the results are written in an audit review file.

- Tracing.

  - Tracing allows the auditor to tag specific live input transactions and to monitor the tagged transactions as they are being processed by the production program.

- Others.

  - The internal EDP auditor should perform pointer reference validity checks to verify that the pointers in the data base records point to valid and appropriate records and that all the pointers, or links, in chained files and data bases actually exist.

6. ADMINISTRATIVE CONSIDERATIONS

- To ensure that the controls and safeguards are effective in preventing, deterring, or detecting unauthorized or fraudulent systems, data, and program access and modification, the controls and safeguards must be administered and audited carefully and continually.

- The administrative and audit considerations will now be considered.

  - The role of the data base administrator.

- The role of the computer security officer.

- The role of the local security officers.

- Administration of user identification and authentication.

- Administration of authorization.

- Administration of surveillance.

- Data bases are used by many departments and are processed by numerous production programs. It is therefore necessary that someone be responsible for the data bases and that someone coordinate the activities that affect the data bases.

  - This, in essence, is the role of the data base administrator.

- The data base administrator may be responsible for the design of the data base organization and the data definitions.

  - He is responsible for controlling and coordinating the use of the data bases by the various users and the production of programs.

  - He is also responsible for designing and implementing procedures to ensure that the integrity of the data bases is maintained.

  - Depending upon the variety of data base users and the company's management philosophy, the data base administrator may review and approve all requests for authorizations.

    . Alternatively, user management or others may control authorizations.

- The computer security officer is responsible for overall computer security.

  - In most organizations, he may be the only person who has access to the authorization mechanisms and the only one who can change the user, terminal, or program authorizations to access and perform specific functions on the data and programs.

  - The computer security officer is responsible for investigating all security violations and for reviewing the surveillance logs to ensure that the security system is functioning properly and to detect emerging patterns of security violations.

  - He is responsible for doing everything he can to enhance the security of the system and maintain it at a prudent level.

- Local security officers are responsible for maintaining physical and administrative security in their particular locations.

  - They are typically located in places with terminals.

  - They are responsible for investigating all security violations that occurred in their locations and for being alert to security violation attempts.

  - If a terminal keyboard is locked by the system as a result of suspected security violation attempts, the local security officer is responsible for investigating the attempt and unlocking the terminal.

  - If there are any terminals in his location reserved for special use, such as on-line programming or sensitive data and transaction processing, the local security officer is responsible for ensuring that such terminals are used by authorized people to perform only the special function.

- User management, users, the computer security officer, and others may be responsible for the administration of user identification and authentication.

  - User management must identify the users whom they have authorized to use the terminals.

    . This may be performed with the assistance of the computer security officer who may explain the implications of authorizing an employee to access the computer system.

  - Users are responsible for properly protecting their user identification and authentication mechanism (i.e., something known, something possessed, or something about the user) against possible compromise.

    . Users are also responsible for notifying the computer security officer whenever they suspect that their user identification or authenication may have been compromised.

  - The computer security officer is responsible for making sure that users understand the need to protect the security of their user identification and authentication.

    . He is responsible for maintaining the user identification and authentication files; for secure distribution of any cards, badges, keys, or passwords; for changing passwords regularly, if passwords are used; and following up on all security violation attempts that involved user identification and authentication.

  - The EDP auditor should, through observation and interviews, check on compliance with security regulations.

- He should be concerned that the user identification and authentication be handled in a secure manner by the user and the computer security officer, that the user properly understand the need to secure the information or object, and that the distribution of the information or object be secure.

- The responsibility for the administration of authorization may lie with user management, the data base administrator, or the computer security officer.

- It is often the responsibility (even if the duties are delegated) of user top management to designate which employees can enter particular transaction types and which can read, write, or modify particular data files and data bases and execute programs.

  - However, it is the computer security officer's responsibility to ensure that management has a clear understanding of what it is they are actually doing or delegating and of the implications of the authorization decisions.

  - The computer security officer might help management understand authorization by preparing written instructions for them and conducting meetings and informal discussions with them.

  - If the computer security officer, during his review of the security log, begins to suspect that the ground rules for designating authorization are being disregarded, he should bring the matter to top management's attention.

7. SUMMARY

- Surveillance is everyone's responsibility. This report discussed how logs and violation reports can be generated. If these logs and reports are not reviewed and attempted security violations are not investigated, their purpose has been

defeated. It is essentially the responsibility of the computer security officer and the internal EDP auditor to verify that proper review and followup are carried out.

B. AN ORGANIZATIONAL REVIEW OF SOME SECURE DATA BASE MANAGEMENT SYSTEMS

- The Air Force Electronic Systems Division sponsored several research and development efforts in the design, specification, and validation of secure data base management systems.

  - Of primary importance are the contributions of System Development Corporation and I.P. Sharp Associates Ltd. Both of these studies helped to identify and clarify the key technical issues in secure data base management technology.

  - MITRE has also developed a prototype security data base management system.

1. THE SDC SECURE DATA MANAGEMENT SYSTEM

- The SDC effort concerned the design of a secure relational data base management system that interfaces with the multilevel environment provided by the secure Multics Operating System.

  - SDC concluded that a relational data base could comfortably exist within the multilevel environment.

  - "The objective of this work was to develop a model and design of the security-related portions of a Data Management System (DMS)."

- The model and design effort focused on those portions of a traditional DMS which are affected by the security constraints of the operating system.

- The result is a design framework which provides the basis for the development of a complete DMS which only has to draw on conventional DMS design technology.

- The mathematical model of a secure DMS encompasses DoD-based security policies which the DMS is to enforce with respect to some of the basic DMS operations.

  - The modeling effort encompasses the modeling of the various levels of the DMS and its operating system interface.

- The modeling work suggested a design for a relational data management system that interfaces with the multilevel environment provided by the secure Multics Operating System.

  - The design utilizes the protection provided by the operating system in such a manner that the DMS contains no code which has an impact on the security of the data in the system and whose correctness must thus be verified.

  - The DMS is designed according to the principle of least privilege; hence, the DMS operating as part of the user's process has no privileges that are not also afforded the user.

- The DMS described in the SDC work is designed to store data base information in the storage containers provided by the underlying Multics Operating System segments.

. To contain no security-relevant code, the DMS must use a number of unilevel segments, because segments are the smallest unit of protection in secure Multics.

- The SDC work is important because it shows that a secure DBMS can exist on a secure system without any additional security-relevant code.

  . However, the SDC effort does not address the additional flexibility that could be gained if smaller units of data could be efficiently protected.

  . The SDC effort is a good example of a DBMS design around existing secure operating system primitives.

2. THE I.P. SHARP PROTECTED DMS TOOL

- The approach taken by I.P. Sharp is unique in that rather than working from existing kernel designs and primitives, they investigated the design of kernel primitives that would support the implementation of a family of secure data management systems. Kernel in this case is defined as that operating system portion that is not available to users or system programmers except under special or unusual circumstances. Primitives are considered such operations as add, multiply, read, fetch, etc.

  - The primitives identified are referred to as the "DMS Tool." The study shows that the DMS Tool is general enough to apply to data management systems implemented as a dedicated DMS, as an application on a secure operating system, or in a computer network.

- The view of the data in the I.P. Sharp work was relational.

  - The I.P. Sharp study recommended that each relation be assigned a single security level; i.e., the data in each relation must be considered at one level.

- Data from several levels cannot be gathered into a single relation and maintain their individual classifications. The resultant relations would have the classification of the most highly classified data that made up the relation.

3. MITRE'S INGRES SYSTEM

- MITRE, working from these past studies, attempted to impose security constraints on the INGRES relational data base management system and to integrate the resultant secure INGRES system with MITRE's UNIX prototype.

  - This effort is important because it was one of the first actual implementations of a secure DMS on a prototype secure operating system.

  - Like the SDC study, the MITRE effort worked with existing kernel primitives to investigate their sufficiency for supporting a secure DMS.

- The approach taken by MITRE was also very similar to the SDC approach in that no security-relevant code was added to the INGRES system. Use was made of the objects provided by MITRE's UNIX kernel to accommodate the relations in an INGRES data base.

- The design of MITRE's UNIX file system, like that of the regular AT&T UNIX, is hierarchical, consisting of directories which may contain other directories or data files.

  - In the MITRE design, data files in a directory assume the same access level as the directory. Consequently, the security level of an INGRES relation (a data file) must be at the same level as its data base (a directory).

- Although this limitation does reduce the convenience of the secure INGRES system, the coordination of INGRES with the MITRE Secure UNIX necessitated the mapping of relations in this manner.

- Adhering to these restrictions, a user is still able to perform multilevel operations on relations in the INGRES data base directory structure.

- In order to use INGRES to process multiple levels of information, the user must create a data base at each security level to be included in the data base.

- Also, a user is able to "read" information from a file at a security level lower than his current level, established at log-in time.

- As a result, a new relation can be created by combining information obtained from relations in data bases at access levels less than or equal to the level of the data base being added to.

C. FUTURE DEVELOPMENTS

- There are two problems that have recurred in the past to much of the secure data base design and implementation work:

  - Often relational data base designs force many relations within a particular program to be at the same level, making data base protection difficult.

  - User interfaces to secure data base management systems are seemingly difficult to design in such a way that the user is not greatly hindered by the security features.

- The solution to the first problem seems to lie in the proper design of security primitives and the implementation of protection features in the right places.

  - For example, a DBMS can rely on the protection primitives provided by the underlying secure operating system or it can, using trusted processes, provide its own protection, possibly at a much finer grain.

  - Currently trusted processes are rather difficult to verify so they are used sparingly. However, as verification technology develops, it will become much easier to design with trusted code.

  - IBM has made a survey of many data base management systems to determine the relationship between operating system and data base system security. Their conclusion is that it is most convenient to separate the design of kernel primitives and DBMS security features.

D. SUMMARY OF DATA SECURITY

- The strategy of securing a data system depends upon seven principles:

  - As many of the protective mechanisms as possible must be removed from the control of the user.

  - Every security-relevant action must be checked before it is permitted to be started.

  - No uncontrolled actions must be permitted after a check has been made ("time-of-check to time-of-use" principle).

  - The principle of "best evidence" holds in EDP security as well as in courtroom law.

- It is not sufficient to check the storage protection keys on the memory block currently in use.

- One has to go back to the basic authorization tables and find out what users possess access privileges to these data and what authority each one has.

- The paramount principle of systems design, "protect the critical function," applies to EDP security.

  - Here the critical function is performed by the security tables, password lists, user directories, and segment access lists.

  - It is essential to ensure that changes be made only by authorized persons and that no unauthorized changes are permitted.

- After a security table has been lawfully altered, a byte count and a hash total should be made of it and stored in encrypted form.

  - Each time the table is consulted, the byte count and hash total of the table should be recomputed, encrypted, and tested against the previously stored values.

- Surveillance and detection provide a fallback defense by affording ex post facto protection.

  - For such protection to be credible, the basic logs used for auditing security-relevant actions, which conceivably could include systems accounting data, should be protected against unauthorized operator or programmer intervention.

  - One way to do this is to record such data on a tape handler whose rewind capability has been disabled.

VI CONCLUSIONS AND RECOMMENDATIONS

VI CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

- Data protection normally implies that the system will protect against data distortion or lost data. It does not imply data will not be lost or distorted, but when a loss does occur, the system user should automatically be notified with the necessary information to recover the data.

- Basically, the areas to be reviewed for data protection would include the following:

  - Terminal error detection capability.

  - Terminal retransmission capability.

  - Terminal receiving buffer media and error recovery capability.

  - Terminal send and receive - computer system error/abnormal detection and recovery procedures.

  - Computer to terminal normal and abnormal selection procedures.

  - General communications protocols.

- Computer system error detection and recovery features - software and hardware.

- Computer system recovery from total failure.

- Computer storage media - data recovery from a major failure.

- Data format editing and validation routines.

- Symbol editing, validation, and control.

- System generated reports defining the reason for failure.

- Development of personnel guidelines for handling system failures.

- Data retrieval procedures.

- Data security is a system provision that allows access to data only by authorized users. Various methods are used to protect data from unauthorized personnel--some simple, some complex.

  - It is a matter of determining the importance of the data under consideration and then developing the necessary data security measures.

  - A few security considerations would include the following:

    . Key words to identify the terminal attempting to access the data.

    . Key words to identify the terminal user.

    . Key words to identify the application program being accessed.

- Key words to identify the data being accessed.
- Use of code words or symbols derived from the data content or numerical value.
- Data scrambling techniques, both on-line and in computer storage.
- Data scrambling and unscrambling key words or symbols.
- Reports to be generated by the system and transmitted to predefined or selected recipients when protected data is accessed.
- Selected sequence of key words--changeable as required--and either manual or automatic.
- Key words to be used by computer operators in order to read data from disk or magnetic tape when loading the system.
- Time of entry and exit key words--symbols used for access and the terminal and/or operator would be identified in a generated report.
- Possible breakdown of the application program into subroutines requiring identifiers.

• The logical methods of maintaining privacy and security are based on access limitations of data processing and telecommunications systems.

- These include the use of passwords, access keys, user IDs, terminal IDs, and operator-entered authorization codes.

- The critical item is that almost all authorization coding must be in the format of the inquiry being made into the data base.

- This format can be used extensively to identify who is trying to gain access as well as where the access attempt is being made from.

- Even if unauthorized users gain information on the access codes, they can be forced to use physical terminals which can be kept under total visual surveillance.

B. RECOMMENDATIONS

- Security is an involved, complex issue, but no organization needs or would want to implement everything discussed in this report. The magnitude of such an effort, to say nothing of the costs, would probably preclude such action.

- In considering data encryption as a security tool, it is important to recognize that since all codes can eventually be broken, it is really a matter of what level of protection the user desires.

- Since the costs of the NBS DES standard on a semiconductor chip is less than $300, it would certainly be advantageous to adopt this standard in-house wherever feasible.

- The trend in security seems to be toward more, not less; more sophistication is becoming the rule. Keeping it simple is becoming more difficult with the passage of time.

  - "Hackers" are creating some problems, but the true extent of their efforts can only be guessed.

- "Hacking" does serve a userful purpose by making corporate executives aware of a problem in their telecommunications and IS.

- Security methodology should, wherever possible, be matched to the level of security required to meet reasonable levels of threat.

- Recognize that by determining that you need some form of encryption, the effective throughput, even on telecommunciations point-to-point circuits, will be decreased.

- One method of maintaining physical security in a telecommunications environment is to implement a private communications facility. It's worth looking in to if security is a serious issue.

  - This approach limits access to entire physical facilities.

  - It also allows the user to better control the physical components over which information is transmitted.

    . That level of control does not exist in the public network.

- The federal government has passed a number of laws curtailing potential user dissemination of privacy information. It is the manager's obligation to be aware of the contents of those laws and to strictly enforce them on his subordinates and their work environment. This includes not only corporate privacy, but individual personal privacy as well.

- Failure to protect individual privacy is considered an "act of omission" by law and is, under federal statute, punishable by imprisonment or a fine, or both. That is a point worth remembering.

APPENDIX A: SOFTWARE SECURITY PACKAGES

APPENDIX A: SOFTWARE SECURITY PACKAGES

- SECURE/IMS - Chicago Data Systems.

  - A teleprocessing security monitor for IMS, where management can select the exact level of security desired. Runs on IBM and IBM-compatible systems; e.g., Amdahl. Price: contact vendor.

- Programmed Cryptographic Facility - IBM.

  - Uses the Data Encryption Standard (DES) and provides a key-generator utility for encryption and decryption. Works in conjunction with the ACF/VTAM Encrypt/Decrypt feature to provide data security over communications lines. Price: $250 per month plus.

- Super MSI (Multiple Systems Integrity Facility) - Allen Services.

  - For use where IBM systems are used to access shared DASD. It also improves systems performance and operates under OS, OS/VS1, SVS, and MVS. Price: $10,000 license fee - lease $625 per month.

- IMS/VS User Security - IBM.

  - Provides IMS/VS users with a means to protect sensitive data by allowing access to authorized users only. Runs on S/370 or above (303X, 308X, etc.) under OS/VS1 or OS/VS2. Price: $150 per month plus.

- ACF 2 - Cambridge Systems Group.

  - Provides the ability to control computer system access and access to its data by specifying algorithmically the access rules for controlled sharing of data. Runs on IBM S/370 and 303X or compatible systems under MVS or VS1. Price $2,700 license fee - lease is available.

- SAFEGUARD II & III - Software Solutions, Inc.

  - Provides a proprietary table look-up algorithm for encrypting data, using pseudo-random number generators and user-supplied keys. Runs under OS/VS, DOS/VS, and DOS using FORTRAN, COBOL, PL/1, or Assembler. SAFEGUARD III uses the NBS DES-standard algorithm. Price: $650 license fee.

- CRYPTOPAK - Computation Planning, Inc.

  - CRYPTOPAK provides exact software emulation of the 56-bit DES along with a 128-bit key byte stream encryptor. Strong algorithm and long-key encryption provide a high level of privacy and security to data and communications links. It runs on IBM/OS and Univac EXEC 8. Price: $9,750 license fee.

- Security Access Controller - EDS.

  - An integrated data security package to control access to system resources. It provides two levels of security: system entry protection for job submission and class and priority usage. It runs on IBM OS,VS1, and MVS. Price: $15,000 license fee.

- Secure - Boole & Babbage.

  - Handles system access and can automatically audit accesses to generate records and data use patterns. It runs on OS, OS/VS1, SVS, and MVS, and provides a ROSCOE interface. Price: $12,600 license fee - lease is available.

- Shared Dataset Integrity (SDSI) - Duquesne Systems Inc.

  - A generalized facility for multiple CPU environments. It provides data set integrity and generates statistics on jobs running, reserves being issued, etc. It runs on IBM OS, VS1, and MVS. Price: $12,000-$15,000 license fee.

- Shared Data Set Integrity (SDSI) - Software Module Marketing Inc.

  - Uses a control file on shared DASD to accomplish inter-system communication. By using ENQ/DEQ requests, which are issued on a local basis, all attached systems are aware of what resources are globally allocated. It runs on MVS and VS1. Price $12,000-$15,000 license fee - lease is available.

- NBS Data Encryption Algorithm - Gamma Technology.

  - This system uses the NBS DES algorithm to secure confidential or proprietary data being transmitted over common carrier facilities. It runs on Eclipse RDOS or AOS systems. Price: $500 license fee.

- NCODE/DCODE - Applied Software Inc.

  - Encrypts and decrypts data and allows information to be encrypted selectively using data within a record or the record position within a data set. It runs on OS and OS/VS1. Price: $70 per month lease.

- Sentry - Sperry Univac Division.

  - Designed for use on the Sperry 1100 series of computers, it handles creation and maintenance of a security data base. Price: $550 per month lease.

- TSO/VS2 Programming Control Facility - IBM.

  - Enhances TSO command facilities by allowing multiple commands to be entered on a single line. It generates detailed utilization statistics and provides an additional functional base within TSO/VS2 to control the access level for each authorized user. Price: $200 per month lease.

- RACF - IBM.

  - An IBM product offering that provides a fairly high level of data security and generates numerous user-related activity reports to permit monitoring of systems parameters, equipment usage, resource allocations, etc. Price: contact vendor.

APPENDIX B: HARDWARE SECURITY APPLIANCES

APPENDIX B: HARDWARE SECURITY APPLIANCES

- IBM 3848 Cryptographic Unit - IBM.

  - Part of the IBM Cryptographic Subsystem, the 3848 hardware extends data control and protection to data communciations terminals and links that speed information from one location to another. It does this by scrambling data before it is stored or transmitted, using encryption techniques. Encryption and decryption are done automatically and without intervention by either the terminal user or by the application. Since the encryption algorithm is implemented directly in a channel attached unit (the 3848), the encryption process can be isolated from host processor storage. The system operates under OS/VS2 (MVS), uses systems network architecture (SNA), and can use the ACF/VTAM Encrypt/Decrypt feature on version 2 (or higher) of ACF/VTAM.

- Numerous companies make, sell, or otherwise distribute all types of locks for terminals, modems, telephones, etc.; hold-down devices of major equipment modules and numerous techniques for otherwise resisting tampering or unauthorized removal have been developed.

  - The best source of such devices is usually the hardware vendor or the supplier of computer room supplies.

  - There are so many of these companies and the volatility of the industry means that so many come and go that it's difficult to list specific supplies or their vendors.

- Your mainframe provider is the best source of information on what to buy and where to get it--almost always from local sources.

APPENDIX C: QUESTIONNAIRE

APPENDIX C
QUESTIONNAIRE

1. Do you currently have any type of security system in your data processing or communication environment?

   Yes _____ No _____

   Can you briefly describe its non-sensitive features? _____

   _____

2. If you don't have a security system, how do you protect against unauthorized access or unwarranted intrusions?

   _____

   _____

3. What software security packages do you now have? _____

   _____

   How do you like it/them? _____

   Which ones are you planning to acquire and approximately when?

   _____

   _____

4. What hardware or other physical security restraints are used in your environment?

   Type_____ Make _____

   How well do they work? _____

   _____

5. Who is responsible for security in your installation and how was that person selected?

_____

_____

6. To whom does the security function report and how often? _____

_____

7. Do you have a disaster recovery plan or a contingency plan in the event of systems failure?

_____

Does it work? _____

When was it last tested? _____

8. Do you now use or are you planning to use the NBS DES?

Yes _____ No _____

If its being used, for how long has it been in effect _____

What does it not cover? _____

9. Who maintains the security system and how often is it evaluated?

_____

_____

10. If you could do it all over, how would you restruct the security system?

_____

_____

_____